ICLG

The International Comparative Legal Guide to:

Data Protection 2019

6th Edition

A practical cross-border insight into data protection law

Published by Global Legal Group, with contributions from:

Addison Bright Sloane
Anderson Mori & Tomotsune
Ashurst Hong Kong
Assegaf Hamzah & Partners
BEITEN BURKHARDT
Bird & Bird
Christopher & Lee Ong
Çiğdemtekin Çakırca Arancı Law Firm
Clyde & Co
Cuatrecasas
Deloitte Legal Shpk
DQ Advocates Limited
Drew & Napier LLC
Ecja Abogados
FABIAN PRIVACY LEGAL GmbH
GANADO Advocates
Herbst Kinsky
Rechtsanwalte GmbH
Herzog Fox & Neeman
Infusion Lawyers
Integra Law Firm
KADRI LEGAL
King & Wood Mallesons
Koushos Korfiotis
Papacharalambous LLC
Lee and Li, Attorneys At Law
Lee & Ko
LPS L@w
Lydian
Matheson
Mori Hamada & Matsumoto
Morri Rossetti e Associati
Studio Legale e Tributario
Nyman Gibson Miralis
OLIVARES
Osler, Hoskin & Harcourt LLP
Pestalozzi Attorneys at Law
Rato, Ling, Lei & Cortés – Advogados
Rossi Asociados
Rothwell Figg
S. U. Khan Associates
Corporate & Legal Consultants
Subramaniam & Associates (SNA)
thg IP/ICT
Vaz E Dias Advogados & Associados
White & Case LLP
Wikborg Rein Advokatfirma AS
## General Chapters:

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Title</th>
<th>Authors/Partners</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>The Rapid Evolution of Data Protection Laws</td>
<td>Dr. Detlev Gabel &amp; Tim Hickman, White &amp; Case LLP</td>
</tr>
<tr>
<td>2</td>
<td>The Application of Data Protection Laws in (Outer) Space</td>
<td>Martin M. Zoltick &amp; Jenny L. Colgate, Rothwell Figg</td>
</tr>
<tr>
<td>3</td>
<td>Why Should Companies Invest in Binding Corporate Rules?</td>
<td>Daniela Fabian Masoch, FABIAN PRIVACY LEGAL GmbH</td>
</tr>
<tr>
<td>4</td>
<td>Initiatives to Boost Data Business in Japan</td>
<td>Takashi Nakazaki, Anderson Möri &amp; Tomotsune</td>
</tr>
</tbody>
</table>

## Country Question and Answer Chapters:

<table>
<thead>
<tr>
<th>Country</th>
<th>Title</th>
<th>Authors/Partners</th>
</tr>
</thead>
<tbody>
<tr>
<td>Albania</td>
<td></td>
<td>Deloitte Legal Shpk: Ened Topi &amp; Emirjon Marku</td>
</tr>
<tr>
<td>Australia</td>
<td></td>
<td>Nyman Gibson Miralis: Dennis Miralis &amp; Phillip Gibson</td>
</tr>
<tr>
<td>Austria</td>
<td></td>
<td>Herbst Kinsky Rechtsanwälte GmbH: Dr. Sonja Hebenstreit</td>
</tr>
<tr>
<td>Belgium</td>
<td></td>
<td>Lydian: Bastaan Bruyndonickx &amp; Olivia Santantonio</td>
</tr>
<tr>
<td>Brazil</td>
<td></td>
<td>Vaz E Dias Advogados &amp; Associados: José Carlos Vaz E Dias</td>
</tr>
<tr>
<td>Canada</td>
<td></td>
<td>Osler, Hoskin &amp; Harcourt LLP: Adam Kardash &amp; Patricia Kosseim</td>
</tr>
<tr>
<td>Chile</td>
<td></td>
<td>Rossi Associados: Claudia Rossi</td>
</tr>
<tr>
<td>China</td>
<td></td>
<td>King &amp; Wood Mallesons: Susan Ning &amp; Han Wu</td>
</tr>
<tr>
<td>Cyprus</td>
<td></td>
<td>Koushos Korfiotis Papacharalambous LLC: Loizos Papacharalambous &amp; Anastasios Kareklas</td>
</tr>
<tr>
<td>Denmark</td>
<td></td>
<td>Integra Law Firm: Sissel Kristensen &amp; Heidi Hojmark Helvge</td>
</tr>
<tr>
<td>France</td>
<td></td>
<td>Clyde &amp; Co: Benjamint Potier &amp; Jean-Michel Reversac</td>
</tr>
<tr>
<td>Germany</td>
<td></td>
<td>BEITEN BURKHARDT: Dr. Axel von Walter</td>
</tr>
<tr>
<td>Ghana</td>
<td></td>
<td>Addison Bright Sloane: Victoria Bright</td>
</tr>
<tr>
<td>Hong Kong</td>
<td></td>
<td>Asharst Hong Kong: Joshua Cole &amp; Hoi Tak Leung</td>
</tr>
<tr>
<td>India</td>
<td></td>
<td>Subramaniam &amp; Associates (SNA): Hari Subramaniam &amp; Aditi Subramaniam</td>
</tr>
<tr>
<td>Indonesia</td>
<td></td>
<td>Assegaf Hanshah &amp; Partners: Zacky Zainal Husein &amp; Muhammad Iqsan Sirie</td>
</tr>
<tr>
<td>Ireland</td>
<td></td>
<td>Matheson: Anne-Marie Bohan &amp; Chris Bolland</td>
</tr>
<tr>
<td>Isle of Man</td>
<td></td>
<td>DQ Advocates Limited: Sinead O’Connor &amp; Adam Kilip</td>
</tr>
<tr>
<td>Israel</td>
<td></td>
<td>Herzog Fox &amp; Neeman: Ohad Elkeslassy</td>
</tr>
<tr>
<td>Italy</td>
<td></td>
<td>Merri Rossetti e Associati – Studio Legale e Tributario: Carlo Impalà</td>
</tr>
<tr>
<td>Japan</td>
<td></td>
<td>Mori Hamada &amp; Matsumoto: Hiromi Hayashi</td>
</tr>
<tr>
<td>Korea</td>
<td></td>
<td>Lee &amp; Ko: Kwang Bae Park &amp; Hwan Kyoung Ko</td>
</tr>
<tr>
<td>Kosovo</td>
<td></td>
<td>Deloitte Kosovo Shpk: Ardiex Rekha</td>
</tr>
<tr>
<td>Luxembourg</td>
<td></td>
<td>thg IP/ICT: Raymond Bindels &amp; Milan Dans</td>
</tr>
<tr>
<td>Macau</td>
<td></td>
<td>Rato, Ling, Lei &amp; Cortés – Advogados: Pedro Cortés &amp; José Filipe Salreta</td>
</tr>
<tr>
<td>Malaysia</td>
<td></td>
<td>Christopher &amp; Lee Ong: Deepak Pillai &amp; Yong Shih Han</td>
</tr>
<tr>
<td>Malta</td>
<td></td>
<td>GANADO Advocates: Dr. Paul Micallef Grimaud &amp; Dr. Luke Hili</td>
</tr>
<tr>
<td>Mexico</td>
<td></td>
<td>OLIVARES: Abraham Diaz Arceo &amp; Gustavo A. Alcocer</td>
</tr>
<tr>
<td>Niger</td>
<td></td>
<td>KADRI LEGAL: Oumarou Sanna Kadrini</td>
</tr>
<tr>
<td>Nigeria</td>
<td></td>
<td>Infusion Lawyers: Senator Iyere Ihenyen &amp; Rita Anwiri Chindah</td>
</tr>
<tr>
<td>Norway</td>
<td></td>
<td>Wikborg Rein Advokatfirma AS: Line Coll &amp; Emily M. Weitzenboeck</td>
</tr>
<tr>
<td>Pakistan</td>
<td></td>
<td>S. U. Khan Associates Corporate &amp; Legal Consultants: Sarifullah Khan &amp; Saeed Hasan Khan</td>
</tr>
<tr>
<td>Portugal</td>
<td></td>
<td>Cuatrecasas: Sónia Queiróz Vaz &amp; Ana Costa Teixeira</td>
</tr>
</tbody>
</table>
PREFACE

It is a pleasure to have been asked to provide the preface to The International Comparative Legal Guide to Data Protection 2019. This edition contains an introductory chapter from White & Case LLP, which briefly charts the technological changes that have driven the evolution of data protection laws in recent decades, and reviews the major challenges that businesses face in complying with the EU’s General Data Protection Regulation in particular. It also explores some of the most significant developing trends in privacy laws globally, and illuminates some of the key policy choices that governments will need to consider as they seek to strike a balance between the right to privacy and the development of data-driven economies. Three further general chapters analyse, respectively, the application of data protection law in outer space; the use of binding corporate rules; and data business activities in Japan – illustrating the far-reaching impact of this field of practice.

The guide provides 42 country question and answer chapters, focusing on key privacy and data protection compliance issues under local laws in countries around the world. This year, new chapters have been added for Albania, Denmark, Ghana, Indonesia, Kosovo, Malaysia, Niger and Pakistan, which reflects the growth of privacy compliance requirements and challenges in an increasing number of jurisdictions worldwide. As with other entries in the ICLG series, this edition will provide a go-to resource for anyone seeking practical guidance on these complex international legal issues.

Tim Hickman
Partner
White & Case LLP
Introduction

Privacy and data protection laws have changed markedly over the last two decades. The highly networked and interconnected world in which we live today was merely a glimmer on the horizon in the mid-1990s. The internet itself was still a fairly new innovation to many people. Many businesses did not yet have public websites. Concepts such as online social media platforms did not exist – and certainly nobody had considered how they should be regulated. Smartphones, wearable technology and artificial intelligence have all made vast leaps over the last 20 years – all driven by new ways of obtaining and processing data. Consequently, courts and regulatory authorities have increasingly had to adapt ageing data protection laws to fit an ever-changing world for which they simply were not designed.

Developments in the EU – the GDPR and Beyond

Policymakers are being forced to design privacy and data protection laws that are flexible, in order to allow for unforeseen advancements in technology. It is in this context that the European Union drafted and finalised Regulation (EU) 2016/679 (the “GDPR”). The GDPR marks the biggest single shift in data protection laws in Europe since Directive 95/46/EC (the “Directive”) was finalised in 1995. Enforcement of the GDPR began on 25 May 2018, marking the end of a four-year legislative process and a subsequent two-year grace period. It introduced a raft of sorely needed clarifications and updates, designed to carry EU data protection law forward, well into the next decade. It also introduced major changes to the compliance burden borne by businesses.

It is difficult to overstate the importance of the GDPR. First, it is extremely wide-ranging. The GDPR retains the Directive’s expansive definition of “personal data", which continues to include all information that relates to any living individual who is identified or identifiable from that information, whether in isolation or in combination with any other available information. This means that almost every business needs to engage in the processing of personal data (e.g., every time an email is sent or received). For many businesses, the GDPR impacts almost every area of operations, from marketing to IT, from human resources to procurement. Anywhere that information about people is handled, the GDPR follows close behind.

In addition to having a wide subject-matter scope, the GDPR has an extremely broad territorial scope. It explicitly applies to businesses that are located in the EU, as well as businesses located outside the EU that: (i) offer goods or services to individuals in the EU; (ii) monitor the behaviour of individuals in the EU; or (iii) are established in a place where EU law applies by virtue of public international law (e.g., various overseas territories of EU Member States will fall within this scope).

Mere accessibility of products or services within the EU does not constitute “offering” for these purposes. However, if a business customises any of its products or services for individuals in an EU Member State (for example, by providing a webpage in a local EU language that would not otherwise be used; by using a local EU top-level domain, such as .eu, .fr or .de; by allowing payment in local currencies such as the euro; and/or by mentioning individuals in the EU) then it is likely that EU regulators would consider that the product or service is being “offered” to individuals in the EU, triggering the application of the GDPR. Likewise, “monitoring”, for these purposes, relates to the behaviour of individuals insofar as their behaviour takes place within the EU (e.g., location tracking of individuals; or tracking individuals on the internet, including subsequent profiling, particularly to take decisions concerning such an individual for analysing or predicting that individual’s personal preferences, behaviours and attitudes, would amount to monitoring). In summary, if a business (even one based outside the EU) wants to interact with individuals within the EU, then it needs to do so in compliance with the GDPR.

Second, the GDPR carries serious penalties. EU legislators and regulators have expressed the view that, for too long, businesses have not taken their data protection compliance responsibilities seriously enough. The challenge has been that the cost of compliance with EU data protection law is undeniably high. Implementing all of the right processes, procedures, policies and agreements requires time, effort and expertise, none of which come cheaply. Conversely, the risk of enforcement has historically been relatively low. EU regulators generally have limited resources that are significantly stretched, and enforcement in respect of every breach is simply not feasible. The introduction of the GDPR has stretched these resources further, as regulators have had to deal with a wave of new data breach reports from businesses. They have also faced increased competition for competent data protection practitioners, from private companies that are increasingly eager to hire experienced advisors.

In addition, in the event that penalties are issued in respect of a breach of EU data protection law, the level of such penalties was comparatively low under the Directive. When considered in the light of penalties for breaches of competition law or financial regulatory law, EU data protection penalties have, in the past, seemed trifling by comparison. The GDPR provided an opportunity to redress this balance. While there was little prospect of reducing the cost of compliance or increasing the frequency with which
penalties could be applied, there was clearly scope to ensure that the severity of the penalties could be increased. After much negotiation, the EU settled on a dramatic increase of the maximum penalties for non-compliance under the GDPR, to the greater of €20 million, or four per cent of worldwide annual turnover – numbers that are specifically designed to attract C-Suite attention.

Third, the GDPR has raised the bar for compliance significantly. It requires greater openness and transparency – the level of detail that businesses are required to disclose in policies and notices regarding their processing activities has significantly increased. The GDPR imposes tighter limits on the use of personal data, especially in the context of direct marketing and certain types of profiling, against which individuals are granted an automatic right to object. Lastly, the GDPR grants individuals more powerful rights to enforce against businesses. Some of these rights (e.g., the right of individuals to gain access to their personal data, and to be informed about how those data are being used) are simply expansions of rights that existed under the Directive, and can largely be addressed without major changes to existing compliance measures. Others (such as the “right to be forgotten”, which permits individuals to require businesses to erase their personal data in certain circumstances, or the right to data portability) were introduced by the GDPR, and require fresh thinking from businesses.

Satisfying these requirements has proven to be a serious challenge for many businesses. Indeed, even if a business has all of the right systems, procedures, policies and agreements in place, and has provided all appropriate training to its employees, it cannot guarantee that none of those employees will ever depart from that training and place the business in breach of the GDPR. In addition, no matter how good a business’s cybersecurity measures are, it can never guarantee that no third parties will be able to gain unauthorised access to personal data on its systems. As a result, businesses are well advised to think of GDPR compliance as an exercise in continually identifying and addressing compliance risks. For as long as new technologies continue to provide us with new ways to use data, this process of spotting data protection risks and working out how to solve them will remain ongoing. It should also be noted that each EU Member State has passed its own GDPR implementation measures, meaning that there continue to be some national variations from one EU Member State to the next.

Beyond the GDPR, the EU continues to issue new laws that impact privacy and data protection. The first of those laws is the Directive on security of network and information systems (the “NIS Directive”), which imposes minimum cybersecurity standards on operators of essential services (i.e., services that are structurally or economically important) and digital service providers (which includes all providers of online services and platforms). Businesses falling within these categories are required to take steps to ensure that their cybersecurity arrangements meet certain minimum thresholds. In the event of a data breach, these businesses will also be subject to mandatory data breach reporting obligations.

Looking to the future, the EU is in the process of finalising the ePrivacy Regulation – a law that will replace the existing ePrivacy Directive, and provide new rules regarding a range of topics, including electronic direct marketing and the use of cookies and similar technologies. While the final text of the ePrivacy Regulation is still some way off, it is clear that the direction of travel is towards a law that will impose much tighter restrictions on the ability of businesses to track individuals using cookies, or to market to them via electronic means. For many businesses, the ePrivacy Regulation is expected to cause a significant upheaval to current approaches to digital marketing and advertising.
of data within the bloc. However, in a number of other parts of the world, data localisation laws are becoming increasingly popular, and in some cases are being used as a means of digital protectionism.

Future Uncertainty

Perhaps the greatest area of future uncertainty at the time of writing continues to be Brexit. While it clearly caries the capacity for uncertainty across a broad range of topics outside privacy, its impact on privacy should not be underestimated. The UK was involved in the drafting of both the Directive and the GDPR, and has had significant input into the preparation of regulatory guidance issued by EU regulators in the last 20 years. But once the UK formally ceases to be an EU Member State, it will become a “third country” for the purposes of EU law. In particular, the UK will not automatically be treated as having sufficiently protective data protection laws to justify the transfer of personal data from the EU to the UK without the need for additional protections.

For its part, the UK has implemented the Data Protection Act 2018, which replicates the relevant facets of the GDPR in full, meaning that there will, in principle, be complete equivalency between data protection laws that apply in the EEA and data protection laws that apply in the UK, after Brexit. In addition, it is unlikely that the UK will impose meaningful barriers to the transfer of personal data from the UK to the EU after Brexit. However, as noted above, it is the transfer of data in the opposite direction (from the EU to the UK) that is likely to pose a thornier challenge.

One obvious way out of this dilemma would be for the European Commission to grant the UK an adequacy decision. On the one hand, this seems like a logical outcome, since the UK will have essentially identical data protection laws to the EU, and is therefore arguably the jurisdiction that is most deserving of an adequacy decision, from a purely legal analysis perspective. On the other hand, it is not yet certain whether the UK will be granted an adequacy decision because, from a political perspective, a large amount remains to be decided in the course of the Brexit negotiations. In particular, the UK’s approach to surveillance and counterterrorism, the active and in-depth collection and retention of communications data in the UK for security purposes, and the UK’s membership of certain international intelligence-sharing organisations, have led to suggestions from some quarters that, after Brexit, the UK’s approach to privacy and data protection will no longer be consistent with the EU’s, making the granting of an adequacy decision more complex than it might first appear.

A further area of uncertainty is the manner in which the GDPR will be enforced. Although the GDPR has now been in force for almost a year, regulatory trends are still crystallising and remain uncertain in the long term. While the mechanisms for enforcement, and the powers of the regulators, are reasonably clear, there is significant doubt in some areas. First, Article 83 of the GDPR (which sets out the maximum penalties applicable to certain types of breaches under the GDPR) is silent on the issue of who can receive penalties under the GDPR. Whereas the Directive explicitly refers to powers used to admonish controllers, the GDPR appears to leave open the possibility that penalties could be applied to both controllers and processors, where they are involved in a breach of the GDPR. This change has serious implications for service provider businesses that act as processors, which were previously relatively insulated from the risk of regulatory enforcement under the Directive.

However, the potential compliance risk under the GDPR goes one step further. Article 83 refers to the concept of an “undertaking”, for the purposes of calculating penalties based on percentages of turnover. An “undertaking” is a concept taken from EU competition law, and essentially means a “business unit” regardless of form or structure. While the analysis can be complex, and is heavily fact-dependent in each case, the term “undertaking” has the capacity to capture an entire corporate group or business arrangement. This means that a breach of the GDPR by a small subsidiary could, in some cases, result in a fine based on a percentage of the entire corporate group, not just the turnover of the entity that committed the breach. In addition, it is unclear whether the introduction of competition law terminology might allow for the possibility that a parent company could be liable for breaches of the GDPR by its subsidiaries. This possibility exists in EU competition law, but there is no clear case law on whether liability could flow up the corporate tree in the same way, in a data protection context.

Notwithstanding the risks in relation to financial penalties under the GDPR, it also needs to be acknowledged that these penalties are not envisaged as front-line compliance tools. For the most part, EU regulators have indicated that they would prefer to work with businesses to ensure that GDPR compliance is achieved, and that the very large financial penalties will be reserved for especially serious, large-scale or systemic breaches. By taking their GDPR obligations seriously, and ensuring that they put sufficient time and resources into GDPR compliance, it is expected that most businesses will be able to significantly reduce the risk of incurring a financial penalty under the GDPR.

As ever, the greatest area of future uncertainty comes not from the law but from technology. It is reasonable to expect that, in 20 years’ time, today’s technology will look as antiquated as the technology of the mid-1990s looks to us. It follows that today’s laws are likely to suffer the same fate as the Directive – being rapidly overtaken by technological developments, leaving courts and regulators struggling to adapt legal concepts and structures to a world for which they were not designed. But even as we look to the horizon, we can see the coming questions with which we may have to grapple. Will the concept of privacy still hold true in a world where wearable technology allows us to record our every interaction? Will the inexcusable rise of tracking technologies in our internet browsers, in our TVs, in our phones, in our cars, on public transport, and via CCTV (especially when coupled with facial recognition) simply mean that we need to get used to the idea that people are watching what we do? Will individuals continue to freely and publicly share personal data on social media? Is that the price we pay for the convenience afforded to us by new technologies? And what will the rise of AI mean for privacy and data protection? If machines ever learn to think independently, will they demand privacy rights to protect those thoughts? If they do make such demands, how should we respond? While the answers to these, and many other, questions may be unknown at this point, the existence of so many questions strongly indicates that data protection law and policy will continue to be a hotbed of change and innovation for the foreseeable future.

Policy Considerations

Global privacy laws are at a crossroads. To date, these laws have tended to focus heavily on the rights of individuals. The aim has generally been to ensure that individuals’ private lives are protected, and are not unfairly infringed upon by governments and businesses. However, interesting new facets are emerging in discussions about the future direction of policy in this area. On the one hand, there is strong business pressure to allow the free flow of data, as a necessary part of a world in which economic growth is increasingly digital. On the other hand, individuals generally do not like the feeling that they are being spied upon, or that their data are somehow out of their control. The overall approach to this issue in the EU, and certain
other jurisdictions, is now settled for the foreseeable future, but lawmakers in jurisdictions where privacy is an emerging theme (notably the US) have hard decisions ahead of them. A major question is where the right balance should lie between the right to privacy and the ability of companies to monetise data about individuals. On the one side, there is the suggestion that the right to privacy is absolute and inviolable (indeed, in the EU it is referred to as a “fundamental right”). Proponents of this view consider that the right of individual privacy is paramount, and that businesses should be made to work around it – and it is not hard to see why this argument is appealing. Large data breaches and failures of security hit the headlines with alarming regularity and illustrate that many businesses are not investing nearly as much in digital security as they should. Indeed, even where proper and responsible investment has been made, it is often impossible for any business to ensure that no well-funded third-party attacker can get into its systems.

In addition to the problems surrounding breaches of security, businesses are often found to have been less than totally forthcoming with individuals about how their data will be used, and with whom those data will be shared. Those businesses that do provide accurate and complete information on this issue tend to do so in privacy notices that are often challenging for the average person to interpret and apply in the context of their own lives. Consequently, there is sympathy with the idea that governments should set policies that will force businesses to take a much more protective approach to the data they handle.

The counter-argument is that while individuals often indicate in surveys that they are concerned about privacy, their actions and their spending habits reveal something else. When offered the choice between a free service that is funded through personalised advertising based on tracking of the individual user’s behaviour, or a service that is more privacy-friendly but that must be paid for by the users, the free (but privacy-invasive) service has proven overwhelmingly more popular. Individual users have a tendency to express concern regarding their privacy, while continuing to prefer services that are funded through the processing of their personal data. As a result, policymakers have tended to stop short of introducing laws that would outright prohibit the provision of services in exchange for the invasive collection of data, on the basis that to do so would rob individuals of access to services they clearly want to use, even where such access comes at the price of invasive use of their data.

A further policy consideration is rapidly approaching. New technologies, including machine learning, AI and fintech, offer untold benefits in terms of analysis of data and fast, accurate decision-making in tasks that might take a human significantly longer. However, the testing and development of these technologies is often reliant on access to vast pools of data in order to produce meaningful results. Developers are facing hard choices about whether to move their operations to jurisdictions that place fewer restrictions on the handling of data for testing purposes. In addition, once products are operational, many businesses are finding that they face a high regulatory hurdle if they decide to offer their services in jurisdictions with very strict privacy laws. Some businesses have started to take the view that the cost of satisfying such strict privacy compliance obligations is too high to justify, until the product is well-established. As a result, users located in jurisdictions with strict privacy laws are increasingly finding that the latest technologies are not available in those jurisdictions. It is therefore important for all jurisdictions to ensure that they implement privacy laws in a way that does not inhibit creativity and technological development. If they fail to do so, they risk turning their citizens into second-class passengers on the digital journey.

### When Businesses Find Themselves Surrounded by Uncertainty, Where Should They Start?

The key message for businesses is that there is an inexorable move towards a world in which laws and regulations will more tightly restrict the ways in which personal data can be used. Many of these laws and regulations present unknown future risks, and give rise to uncertainty. But commerce is increasingly dependent upon data – businesses that considered themselves to be manufacturers, transportation companies, or supermarkets as recently as five years ago are now finding that their ability to extract value from transactions is ever more reliant upon the availability of accurate data. Caught between a dependence on data, and the risk of laws that restrict the use of such data, businesses should be forward-thinking, and plan ahead.

Businesses should start by identifying and addressing the biggest compliance risks they face under the GDPR and other applicable laws, and should address those risks in order of severity of impact. It is often possible to generate quick wins by meeting easy-to-complete requirements such as the update or creation of privacy policies, notices, contracts with customers and vendors, and other key documentation.

One of the most significant risks is that nobody will take responsibility for data protection compliance unless they are required to do so. Therefore, it is generally advisable to ensure that responsibility for compliance is allocated to someone, and that there is a mechanism for checking on progress. As part of this process, businesses should seek to build awareness of data protection and privacy expectations and requirements among their staff members, and to ensure that the operational impact is well understood by staff who process personal data.

Last, but by no means least, businesses should see this as an opportunity. Lawmakers are taking privacy and data protection seriously because the public increasingly take those issues seriously. A well-planned and well-executed privacy compliance programme can provide a competitive advantage by helping a business to ensure that its customers, suppliers and employees feel confident in allowing that business access to their data – which is increasingly the lifeblood of today’s digital world.
Dr. Detlev Gabel is a partner in the Frankfurt office of White & Case and head of the Firm’s EMEA Data, Privacy & Cyber Security Practice. Detlev advises multinational clients on a broad range of data protection and data security matters, including European and German data protection law compliance, cross-border data transfers and information governance issues.

Detlev frequently publishes and speaks on topics relating to the aforementioned areas. Notably, he is the co-editor and co-author of a treatise on European and German data protection law and lectures on data protection law at the University of Oldenburg, Germany, in a course leading to a Master of IT Law.

The legal directories consistently list him as a leading individual for data protection law in Germany.

Tim advises on all aspects of UK and EU privacy and data protection law, from general compliance issues (such as implementing privacy policies and consent forms) to more specialised issues (such as managing data breaches, structuring cross-border data transfers and complying with the “right to be forgotten”). Tim has a detailed knowledge of the EU’s General Data Protection Regulation, and co-authored White & Case’s Handbook on that legislation (www.whitecase.com/eu-gdpr-handbook).

Clients appreciate Tim’s ability to find pragmatic and commercial solutions to complex (and frequently multi-jurisdictional) data protection compliance questions.

Tim has significant experience of working with a wide range of clients in the EU, the US and Asia. He has spent time on secondment at Google, advising on cutting-edge privacy and data protection issues. He has also spoken at several events at Harvard Law School, and he delivered the closing address at the Harvard European Law Conference 2019.
Chapter 2

The Application of Data Protection Laws in (Outer) Space

Rothwell Figg

1 Introduction

We live in a rapidly changing world, and nothing is evolving faster than the information and communication technologies that have become a part of almost every aspect of our daily lives. While some of us can remember a time without the Internet, smartphones, search engines, and digital assistants – those days are long gone. We live in a digitalised society, and we expect to have the information we want and the ability to control our lives literally at our fingertips – simply by querying Google, by tapping a button on an app, or by asking Siri or Alexa.

Our communications infrastructure and the hardware devices and computer software that comprise it have been transformed into network-connected devices, systems, and services – often referred to as the “Internet of Things” or “IoT” – that are “smart”. “The widespread incorporation of ‘smart’ devices into everyday objects is changing how people and machines interact with each other and the world around them ….” Devices, systems, and technologies, such as smart thermostats, are installed in our homes, and predict our living patterns and temperature preferences. Our smartphones and digital assistants anticipate the information we are likely to want, when we want it; for example, telling us the news we care about before we even know to ask. And instead of our GPS responding to our inquiry for directions, it anticipates where we will likely want to go at a particular time of day based on our past travel, and sends us alerts as to where our car is parked, and how long it will take to get to work based on current traffic.

While the benefits of the aforementioned devices and services to society, to our economy, and to us as individuals are undeniable, “their deployment has also introduced vulnerabilities into both the infrastructure that they support and on which they rely, as well as the processes they guide. Cyber actors have already used IoT devices for distributed denial-of-service (DDoS) attacks, and we assess they will continue. In the future, state and non-state actors will likely use IoT devices to support intelligence operations or domestic security or to access or attack targeted computer networks.”\(^1\) The most significant challenges in addressing such unauthorised access and attacks, and in enforcing data protection laws, rules, and regulations, are the difficulties of dealing with cross-border issues (e.g., cross-border flows of data) and accompanying choice-of-law issues.

The legal system is trying to keep up, but it is doing so based on the constructs of nation states and regional laws; a two-dimensional system with artificial boundaries regulating a three-dimensional boundary-free environment. In today’s world, we regularly travel – across state lines and country lines, across continents and oceans. And as we travel, we generate data about ourselves. We make purchases with credit cards; join WiFi hotspots; use our apps; we tweet; post; talk to Siri and Alexa; wear a fitness tracker or smart watch; check in at the gym; use GPS; use “smart” appliances; shop online; and the list goes on. Trying to determine which data protection laws, rules, and regulations apply to us, and to our data, as we move about the world, is confusing and complex. And even if we as individuals stay put, the data about us travels the world – and beyond. Our home-town gym may contract with a network of other gyms that span the globe, sharing our information across multiple continents and into outer space by transmitting the data via satellite. The benefit to us is that we can go anywhere, and it’s “just like home”. We can go anywhere and stay “connected”. We may not physically be at home, but we can control our “smart devices” remotely, or just let them take control. The drawback to us is that our personal data is processed, who is controlling the collection, transmission and/or processing, and who is doing the collecting, transmitting, and/or processing – is a formidable task even for a seasoned data protection expert. Equally as challenging, from the standpoint of the data controller or processor, is determining in such an ecosystem, what is required for compliance, the metes and bounds of the privacy programme to implement, the incident response programme to employ, and what type of impact assessment is required.

The future will only get more complex unless the legal system adapts and changes. There are simply too many different laws governing – in many cases – the same personal data. According to the United Nations Conference on Trade and Development, as of April 2, 2019 there were 107 countries with (different) legislation in place to secure the protection of data and privacy.\(^2\) In addition, there were at least 14 countries that were in the process of drafting legislation, and there were a number of regional groups that were aimed at unifying the laws of countries in certain regions.\(^3\) However, unlike the GDPR – which displaced the domestic data protection laws of countries in the EU – other regional laws do not displace countries’ domestic laws. For example, in Asia, the Asia-Pacific Economic Cooperation (APEC) Privacy Framework developed uniform data protection laws – called the APEC Cross-Border Privacy Rules (CBPR) system – but unlike the GDPR, the CBPR system does not displace or change a country’s domestic laws or regulations.\(^4\)

Adding further to the complexity of the legal landscape, there are also some laws that are industry-specific. This is especially common in the United States. For example, the Communications Act of 1934 imposes data privacy and security requirements on “cable operators” and “satellite carriers.”\(^5\) And while there are some entities that are governed by a patchwork of data protection laws, others seemingly

\(^{1}\) Jenny L. Colgate

\(^{2}\) Rothwell Figg
fall through the cracks entirely and are governed by none. For example, currently non-profits are exempt from the California Consumer Privacy Act, and international intergovernmental organisations like the European Space Agency (ESA) are exempt from the GDPR. All of this is to say that now may be the perfect time for countries around the globe to discuss a set of global data protection standards. People and companies are only getting more transitory. It is less clear than ever before where a “company” is actually located because often in today’s world a company is a network of individuals working collaboratively from remote locations. And the current landscape of trying to determine where and by whom personal information is collected, transmitted and processed will only get murkier in the future, as the world continues to “grow up” into outer space. Of course, realising the unreliability of a set of global data protection standards, the authors propose that at the very least a new treaty, or new international rules and/or regulations, should be considered addressing data protection laws in outer space.

Space tourism is a growing industry, and while no tourist has been to space since 2009, some are saying that 2019 is the year this is going to change, as a number of private companies, such as Virgin Galactic, Blue Origin, SpaceX, and Boeing, have been working diligently to fulfil promises of taking humans to space. Drones are becoming a part of everyday life. They are used for surveillance (everything from catching lawbreakers, to tracking down pipeline leaks, to monitoring the impacts of climate change on wildlife); they take pictures from the air (such as action photos of extreme sports and property pictures for realtors); they are used to help film Hollywood movies; there are military applications; and some commercial enterprises are even exploring—or implementing—the use of drones to deliver goods to people. In April 2019, Google’s drone delivery service was approved for public use in Australia. It is only a matter of time before drones are used in outer space. Drones are already operating in “near space”—the area between where airplanes safely fly within the “domestic airspace” above the countries below, and where outer space begins.

Also, we have an emerging space infrastructure and the deployment of space and terrestrial components, products, and services that are becoming an essential part of the ecosystem of interconnected devices and services. Companies and organisations are already working to realise the promise of satellite-powered networks that would bring the IoT to everywhere in the world. For example, the “Internet of Things Everywhere on Earth” (IOTEE) Project is a project that has been funded by the European Union to provide IoT Low-Power Wide-Area (LPWA) services from space. As another example, Amazon Web Services (AWS) recently struck a deal with satellite provider Iridium to develop a satellite-based network called CloudConnect, designed specifically for IoT applications, to “bring internet connectivity to the whole planet”. And in October 2018, SemTech and Alibaba Cloud agreed to develop an IoT network in China using small satellites in low Earth orbit.

Global Positioning System (GPS) technology is also an area of growing technological development that involves outer space and data protection issues. GPS involves multiple satellites in the Earth’s atmosphere transmitting signals to devices that can determine the current location on the ground. The satellites began being launched in 1978 and have since grown to a network of 24 global satellites, which give full coverage for GPS navigation everywhere. GPS was originally used by aviation pilots for navigation; then it expanded into expensive road vehicles, followed by inexpensive portable units for vehicles; and today our communication and media devices routinely make use of GPS technology, tracking where you and your personal property are located.

In this chapter, we explore a variety of legal issues that would likely come into play when dealing with the processing of personal data in outer space considering the existing patchwork of regulations and treaties. We also propose that a new outer space treaty should be negotiated, or new international rules and regulations adopted, providing data protection minimum standards and making clear which law(s) govern the collection, use, disclosure, retention, and disposal of personal data or personally identifiable information (PII) in outer space. The space infrastructure and deployment of space and terrestrial components, products, and services is rapidly evolving and, we submit, now is the time to seriously consider making regulatory changes so that our data protection laws are better suited to deal with the future ahead of us.

II A Hypothetical to Explore the Current Regime of Applicable Law

To explain the current situation with the law, we will use a hypothetical scenario—imagine that due to technological advances, a space data-centre start-up has built a space-based data-centre platform that will operate in Low Earth Orbit (LEO) at 58 miles above sea level (8 miles higher than NASA considers “outer space” to begin). (Note: Currently, low earth orbit satellites operate in the first 100-1,200 miles above Earth.) However, “[i]n theory, it is only the horizontal speed which decides whether a satellite goes into orbit”, such that the lower the altitude above earth, the higher the required orbital velocity. The company claims that the benefit of its data-centre over other space data-centres is that due to its proximity to Earth, communication is faster and its services are less expensive. Like other space data-centres, it claims its system of LEO satellites (LEOS) is an alternative to Internet-based data storage and services, which are notoriously insecure. The company seeks your legal advice to ensure that, because it operates in outer space (right at the Karman line), it is not subject to any data protection regulations.

A threshold issue for determining what regulations would apply in outer space is resolving the issue of what is outer space. Where does airspace end and outer space begin? There is currently no internationally agreed upon answer to this question. The most accepted “norm” to define the point at which the airspace above a country ends and outer space begins is a boundary called the Karman line. For decades, the Fédération Aéronautique Internationale (FAI) has set the Karman line at 100 kilometres or 62 miles high. But again, this is not a universal standard, and even the US Air Force and NASA do not abide by this limit; instead, treating the line as 50 miles. In view of the foregoing, it would be difficult to advise the client whether outer space or airspace laws are applicable.

b. Airspace Law

Unfortunately, application of the law only gets more complex from there. A basic principle of international air law, which was affirmed in Article 1 of the Paris Convention on the Regulation of Aerial Navigation (1919) and subsequently by various other multinational treaties, is that every state has complete and exclusive sovereignty over the airspace above its territory, including its territorial sea.

Thus, airspace is generally considered an appurtenance of the
subjec
tant

The aforementioned would suggest that as the LEOS orbit the Earth, so long as they are lower than “outer space” (an undefined boundary), they would be subject to the data protection laws of any country above which they pass over, as well as whatever applicable laws apply to personal data on the High Seas, to the extent they are passing over non-territorial waters. Obviously, ensuring compliance with so many countries’ data protection laws would be unwieldy and impractical. We note that these issues would likely not arise for a geostationary satellite, which stays in one location relative to a specific spot on earth.

There are also a number of airspace treaties that could potentially apply to further address the choice-of-law questions regarding which countries’ data protection laws would apply, particularly in the event of a data breach. For example, historically, when a crime has been committed during an international flight, there have been difficulties pinpointing when and where it occurred and hence in determining which nation’s laws may have been violated (or in the case of violations that occur in airspace over the High Seas, whether there is any applicable law).xxii The same would be true with respect to a data breach of a LEOS. The 1963 Tokyo Convention on Offenses and Certain Other Acts Committed on Board Aircraft provided that in addition to the law of the nation where the violation occurred applying, nations may also extend their criminal law and jurisdiction to aircraft of their registry when they are outside national territory.xxxi Notwithstanding, it is not clear that this convention would even apply to LEOS, as it seems to apply only to manned aircraft. Further, this convention is limited to “offenses against penal law”, and thus would not apply to data protection regulations that impose only civil remedies.

There are also laws and treaties addressing civil offences that occur in airspace, but there is no general principle that the law of the nation of registry of the aircraft applies to all civil offences that occur on board (to parallel the aforementioned Tokyo Convention on criminal acts). Instead, there is a patchwork of international agreements that affect the exercise of civil jurisdiction by nations, and their application to data breaches on unmanned LEOS (as opposed to traditional civil offences on manned aircraft) is as imperfect as the application of the Tokyo Convention discussed above. For example, the 1929 Warsaw Convention for the Unification of Certain Rules Relating to International Carriage by Air applies “to all international carriage of persons, luggage or goods performed by aircraft for reward”, and would presumably not apply to the processing of data by a LEOS.xxxii Additionally, there is a further choice-of-law question to the extent the LEOS pass over the High Seas. Article 92(1) of the United Nations Convention on the Law of the Seas (UNCLOS) provides that ships shall sail under the flag of one state only and “save in exceptional cases expressly provided for in international treaties or in this Convention, shall be subject to its exclusive jurisdiction on the high seas”.xxxi One of the “exceptional cases” identified in Articles 101–107 of the convention concerns piracy. Article 105 provides that “[i]n the high seas, or in any other place outside the jurisdiction of any state, every state may seize a pirate ship or aircraft, or a ship or aircraft taken by piracy and under the control of pirates, and arrest the persons and seize the property on board”. Again, the issue here is that the language of the treaty does not clearly apply to data piracy, where there may be no “pirate ship or aircraft”, and indeed the “pirates” may be located far away from the property (personal data) being seized. The definition of “piracy” in Article 101 similarly is focused on “crews” and “passengers” of ships and aircraft.xxxii

In sum, trying to advise a client regarding the data protection legal framework that would apply to a network of LEOS processing personal data – even assuming it is a given that they are in airspace and not outer space – would be next to impossible, just from a choice-of-law standpoint. There are multitudinous treaties and conventions that could potentially apply, but the applications are stretched and imperfect.

c. Outer Space Law

The application of outer space law to data protection issues is no different.

Outer space law began in 1959, shortly after the Soviet launch of the first artificial satellite into space (Sputnik 1), with the creation of the United Nations Committee on the Peaceful Uses of Outer Space (COPUOS).xxv COPUOS was formed during the “space race” period between the United States and the Soviet Union, with the mission of ensuring that outer space is used for peaceful purposes.xxxvi In 1966, the UN drafted Resolution 2222 (XXI), the “Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies”, also known as the “Outer Space Treaty”. The Outer Space Treaty was founded on similar principles to those of COPUOS, including a recognition of “the common interest in all mankind in the progress of the exploration and use of outer space for peaceful purposes” and “believing that the exploration and use of outer space should be carried on for the benefit of all peoples irrespective of the degree of their economic or scientific development”.xxxvii

The Outer Space Treaty and other similar outer space treaties (e.g., the Space Liability Convention and the Registration Convention) – like the treaties and conventions on airspace and the High Seas – do not cleanly apply to the issues of data protection. They were drafted before the time of data, and do not even begin to contemplate the commercial use of outer space for, inter alia, data processing. Notwithstanding, like the airspace and High Seas treaties, there are some provisions of the outer space treaties that address liability generally, which could arguably be stretched to cover data protection and breaches in outer space.

For example, Article VII of the Outer Space Treaty provides that each State Party to the Treaty that launches or procures the launching of an object into outer space, and each State Party from whose territory or facility an object is launched, is internationally liable for damages to another State Party to the Treaty or to its natural or juridical persons by such object or its component parts on the Earth, in air or in outer space. Presumably, this could mean that a country could be liable to another country, to the extent that an object launched from the first country resulted in a data breach of “juridical persons” of the second country, but only if the data breach would occur by launching an object into space (an unlikely scenario).

Another example of an issue with applying the Outer Space Treaty to data protection is that it seemingly provides for the ability to game the system. Article VIII provides that “[a] State Party to the Treaty on whose registry an object is launched into outer space … shall retain jurisdiction and control over such object, and over any personnel thereof, while in outer space”. In other words, if one’s space-processed data is hacked by another object that is launched into space, then the data protection laws of the country from which the object was launched into outer space would retain jurisdiction over any legal claims relating to the damage. The issue here is that bad actors could potentially avoid legal consequences by simply “launching” (or acting/breaching) from a country where there are no data protection laws. For example, of the 135 countries that are parties to the Outer Space Treaty, 30 countries appear to have no
national data protection laws, and an additional 13 only have draft data protection legislation.\textsuperscript{xvi}

In view of the foregoing, it would be difficult to advise a client of the possible data protection laws that would apply to an outer space data-centre. One could comfortably say that the other space treaties are only concerned with liability. Thus, unless a breach occurs, it is probably fair to say that there are no data protection regulations that extend to outer space. In the event of a data breach, it is possible that the outer space treaties would be stretched to extend domestic data protection regulations to cover the breach, such as by applying the law of the nation where the breaching party resided (even if they did not “launch”) or the law of the nation whose object/data is hacked.

d. Shortcomings of Existing Data Protection Regulations

The aforementioned discussions of international law regarding airspace, the High Seas, and outer space were all concerned with choice-of-law issues, i.e., determining if there is a regulatory framework in place that establishes what law(s) apply. As discussed above, the answer is that for a lot of new technologies – satellites, drones, aircraft, commercial space objects, IOT devices, and so forth – the international choice-of-law rules do not clearly apply. But even if they did clearly apply, there is still another issue, and that is that the domestic data protection laws do not clearly apply outside of Earth.

By our calculation, there are at least 118 countries in the world today with data protection laws in place, and another 19 in the drafting process.\textsuperscript{xviii} Because it is not feasible for us to discuss each of these laws here, we will be focusing on two – the EU’s General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) (which goes into effect on January 1, 2020). For the reasons we explain below, we believe both regulations apply to personally identifiable information processed in outer space, but there is a loophole in the GDPR that could allow companies processing PII in outer space to shirk their otherwise applicable GDPR obligations.

i. GDPR

The territorial scope of the GDPR’s application is broad. It applies to: (1) the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not; (2) the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where processing activities are related to (i) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union, or (ii) the monitoring of their behaviour as far as their behavior takes place within the Union; and (3) the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.\textsuperscript{xxii}

Given the breadth of the aforementioned terms, it is easy to imagine possible scenarios where the GDPR could apply in outer space – for example, a controller or processor that is located in the EU and processes personal data via a satellite located in outer space; satellite Internet, GPS, and media providers that offer their services to customers in the EU; and a space data-centre that is based in the EU or processes data about individuals located in the EU. In all of these situations, the GDPR seemingly applies.

The one area where the GDPR seemingly missteps is with respect to transfers of data to outer space. Chapter 5 governs “[t]ransfers of personal data to third countries or international organizations”. However, Chapter 5 (and the rest of the GDPR) is silent with respect to transfers of data outside of the Earth.

Article 44, the first article of Chapter 5, provides:

Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation. All provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined.\textsuperscript{xxiii}

Thus, even though the territorial limitations of Article 4 of the GDPR are broad enough to cover data processed in outer space, the regulations regarding transfers of data – from Chapter 5 – are limited to transfers on Earth. This means that to the extent an individual engages with a business that is ordinarily subject to GDPR protections, there is a potential loophole that the business could rely on – to the extent it processes data in outer space – to shirk its otherwise applicable GDPR obligations.

ii. CCPA

Our reading of the CCPA is that there is no similar loophole. Section 1798.150 of the CCPA provides a broad obligation on the part of businesses to “implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information”, and provides that, to the extent a third party gains unauthorised access and exfiltration, theft, or disclosure results as a consequence of the business’s violation of its duty to implement and maintain such security procedures and practices, then damages, injunctive or declaratory relief, or any other relief that the court deems proper could result.\textsuperscript{xxiv} Thus, because section 1798.150 applies regardless of where data is being processed – and further because there are no provisions that are limited to transfers of data on Earth – the “outer space loophole” of the GDPR has been avoided.

In sum, this short analysis of the GDPR and the CCPA is just to highlight the fact that the issues with the application of existing regulations to the future of the processing of PII in air and outer-space is not just an international law problem. It is also something that each nation should consider with respect to its own regulations, to ensure that there are no unintended loopholes in its data protection laws that could apply when personal data is processed in outer space.

III Future International Treaty, Rules, or Regulations

Given the above analysis, it is clear to the authors that new international laws, rules, and/or regulations are needed to more clearly establish which data protection laws apply when personal data is processed in air and space. Current international air law and High Seas law addresses criminal and civil law through a patchwork of rules that do not clearly apply to unmanned aircraft or devices processing personal data, and the outer space treaties are concerned only with liability, and arguably do not extend to govern compliance or to establish liability for failures to comply or as a result of data breaches (without corresponding physical altercations). As such, a legal framework – such as in the form of a data protection treaty – should be negotiated, or a set of rules and/or regulatory standards – perhaps under the authority of the International Telecommunication Union (“ITU”)\textsuperscript{xv} – should be drafted applicable to the protection of personal data in airspace above nations, above the High Seas, and in outer space. Such laws, rules and/or regulations could provide much needed clarity to choice-of-law issues and, thus, requirements for compliance, required actions upon a data breach, enforcement and remedies.
In determining the applicable choice-of-law provisions, care should be given to ensure that: (1) objects processing data in airspace/outer space would not be subject to the laws of every nation over which they pass; and (2) the applicable law should not be determined based on a data hacker’s activities (such that hackers could position themselves in a jurisdiction without data protection laws, in order to avoid legal consequences for their actions). Logical choices for which law should apply would be: (1) the law of the country from where the object processing the personal data being hacked is launched or takes off applies; (2) the law of the country in which the entity controlling or processing the data resides applies; or (3) the law of the country the data subjects whose data is being processed resides applies.

Additionally, a treaty (or other rules and/or regulations) should set forth minimum standards for data protection that apply once the data being processed pass a certain threshold (i.e., so as to exclude personal drones and similar devices), to ensure a minimum international standard for data protection in air and space. For example, similar to the treaties on air and outer space, there should be registries to record objects that are processing data in air and space (separate and apart from the registries of objects launched into outer space generally).

Data protection inventory assessments (DPIAs), similar to those required by the GDPR, should also be compulsory in order for persons and entities to process data in outer space (and high airspace, as of a certain altitude). Additionally, a set of minimum requirements governing participating persons’ and entities’ processing of personal data should be specified and certification (or self-certification) should be stipulated in order for entities to process personal data in high air and outer space, similar to the US-EU “Privacy Shield” and white lists/black lists under the GDPR. The adoption of the aforementioned framework would provide for better data protection through design (including a “baseline” set of data protection requirements) and better transparency regarding the types and amounts of data that are being processed in high air and outer space.

Conclusion

The age of personal data is here, and technological advances are shrinking the world we live in – not just two-dimensionally, but up into airspace and outer space, as well. Unfortunately, existing legal frameworks do not sufficiently address which laws apply to personal data in airspace and outer space, and as such, a new international treaty or set of rules and/or regulatory standards is needed to fill this gap, lest there be legal uncertainty which could impede the adoption of innovative technologies. Additionally, nation states should be careful to consider air and space issues when drafting their data protection laws, to ensure that there are no unforeseen loopholes where personal data is processed in outer space.

i. Daniel R. Coates, Director of National Intelligence (appearing before the Senate Select Committee on Intelligence to provide the U.S. intelligence community report on Worldwide Threat Assessment (May 11, 2017)).

ii. Daniel R. Coates, US Director of National Intelligence (appearing before the Senate Select Committee on Intelligence to provide the U.S. intelligence community report on Worldwide Threat Assessment (May 11, 2017)).


v. Id.

vi. “Satellite carriers” are defined as any “entity that uses the facilities of a satellite or satellite service . . . to establish and operate a channel of communications for point-to-multipoint distribution of television station signals . . . .” 47 U.S.C. § 338(k)(7); 17 U.S.C. § 119(d)(6).

vii. See California Consumer Privacy Act of 2018 (applies to “businesses”, and “business” is defined as a legal entity organised or operated for the profit or financial benefit of its owners which meets certain criteria).


xx. Id.


xxii. Id.


xlii. GDPR, Article 3.

xliii. GDPR, Article 44.

xliv. CCPA, section 1798.150.

xlv. See https://www.itu.int/en (accessed April 28, 2019). (ITU is an agency of the United Nations that is responsible for issues concerning information and communications technologies, including: setting standards for technologies (such as 3G and 4G mobile standards, HDTV and other television standards) and coordinated universal time (UTC); coordinating the shared use of the radio spectrum; and creating and maintaining an orbit/spectrum international regulatory framework that, inter alia, seeks to ensure interference-free operation of radiocommunications.)

Martin M. Zoltick has been practising in the field of technology law, focusing on intellectual property matters, transactions, data protection, and privacy, for more than 25 years. A Certified Information Privacy Professional in the United States (CIPP/US), Mr. Zoltick handles matters related to cybersecurity, privacy, and data protection, including working closely with clients to ensure compliance with the evolving legal and regulatory landscape, to establish company best practices, policies, and procedures, and in carrying out privacy-related impact assessments and incident response plans. He has a degree in computer science, worked as a software engineer, and regularly represents entrepreneurs, investors, emerging businesses, middle market, and mature companies in technology and IP-related matters, including securing protection for valuable intellectual property and data, handling transactional matters and due diligence reviews, and serving as counsel in enforcement and defence proceedings.

Jenny L. Colgate is an experienced intellectual property lawyer. She is a Certified Information Privacy Professional in the United States (CIPP/US) and has experience counselling clients on matters related to privacy, data protection, and cybersecurity, as well as litigating cases concerning data misappropriation and related IP issues. Ms. Colgate was named a Washington, DC Super Lawyer “Rising Star” for IP litigation seven years in a row from 2013 to 2019.

Attorneys in Rothwell Figg’s cybersecurity, privacy, and data protection practice – all of whom are Certified Information Privacy Professionals in the United States (CIPP/US) – advise clients on the broad range of issues that businesses face daily in order to secure data, guard valuable intellectual property, and comply with the laws, rules, and regulations regarding privacy. We work closely with clients to recognise, respond to, and minimise the serious risks associated with the collection, use, retention, disclosure, and disposal of personal information, susceptible IP, and data; and we assist with the design and implementation of cybersecurity and data protection best practices, compliance programmes, and incident response plans to help organisations comply with the evolving data privacy requirements. In the unfortunate circumstance when a company does face a breach, we are well-situated to assist during and in the aftermath of the incident, including taking immediate corrective measures, negotiating with the relevant regulatory authorities, defending against lawsuits arising from breaches, and advising on improvements to the security and privacy programmes for the future. We also have experience successfully representing clients in privacy-related investigations initiated by the Federal Trade Commission (FTC).
Chapter 3

Why Should Companies Invest in Binding Corporate Rules?

FABIAN PRIVACY LEGAL GmbH

© Published and reproduced with kind permission by Global Legal Group Ltd, London

1 Introduction

Article 47 of the EU General Data Protection Regulation ("GDPR") expressly recognises Binding Corporate Rules ("BCR") as one of the means for the international transfer of personal data, both for controllers (covering personal data they control) and for processors (covering personal data they process on behalf of others based on a processing agreement). Before the GDPR came into force, BCR were recognised and approved by the current practice of the data protection authorities and the guidelines of the Article 29 Working Party ("Working Party"). Other countries outside of the EU, such as Switzerland, recognise the concept of BCR as well.

What is the practical significance of BCR for companies and why should companies invest in BCR? This article shall explore what BCR under the GDPR are, what needs to be considered when applying and implementing BCR, and their benefits.

2 What are Binding Corporate Rules?

The GDPR defines the term “Binding Corporate Rules” in Art. 4 para. 20 as “personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity”.

BCR are therefore one of the appropriate safeguards for the transfer of personal data within a group of undertakings, or group of enterprises engaged in a joint economic activity (“Group”) from the European Economic Area ("EEA") to countries which do not provide an adequate level of data protection. In practice, BCR are a set of internal rules, standards and processes, such as codes of conduct, that regulate internal data management practices in a binding and consistent manner throughout the Group, with the primary objective to facilitate the free movement of personal data within that Group while ensuring an effective level of data protection. BCR are, however, not intended to be used as a means for allowing cross-border data transfers to companies which are not part of that Group.

The concept and content of the BCR have mainly remained the same under the GDPR, with some minor changes. One significant change is the extension of the group of applicants. While BCR were previously only applicable to groups of undertakings, they are now also open to groups of enterprises engaged in joint economic activities. The term “group of undertakings” is defined in Art. 4 para. 19 GDPR as a “controlling undertaking and its controlled undertakings”. However, the term “group of enterprises engaged in a joint economic activity” is not defined in the GDPR. The term is open to interpretation, but may be taken to include a group of independent organisations which have agreed to cooperate, such as joint ventures.

In addition, the list of minimum requirements has been extended to include the contact details of each member of the Group, the description of the principles of privacy by design and privacy by default, the right not to be subject to profiling, the information obligations according to Art. 13 and 14 GDPR, and the details of the persons responsible for training and complaint procedures.

The Working Party provides, in WP 256 (BCR for controllers) and WP 257 (BCR for processors), updated guidelines and very useful tables setting out the elements and principles that controllers and processors should state in their BCR, incorporating the new language in line with the GDPR and the necessary content mandated by Art. 47 GDPR, and making a distinction between what must be included in the BCR and what must be presented to the competent supervisory authority in the BCR application.

BCR must comply with a whole range of requirements, and must contain all elements as set out in Art. 47 para. 2 GDPR, including:

a) the structure and contact details of the group of undertakings or group of enterprises engaged in a joint economic activity, and of each of its members;

b) the data transfers or set of transfers, including the categories of personal data, the type of processing and its purposes, the type of data subjects affected and the identification of the third country or countries in question;

c) their legally binding nature, both internally and externally;

d) the application of the general data protection principles; in particular, purpose limitation, data minimisation, limited storage periods, data quality, data protection by design and by default, legal basis for processing, processing of special categories of personal data, measures to ensure data security, and the requirements in respect of onward transfers to bodies not bound by the BCR;

e) the rights of data subjects in regard to processing and the means to exercise those rights, including the right not to be subject to decision based solely on automated processing, including profiling, the right to lodge a complaint with the competent supervisory authority and before the competent courts, and to obtain redress and, where appropriate, compensation for a breach of the BCR;

f) the acceptance by the controller or processor established on the territory of a Member State, of liability for any breaches of the BCR by any member concerned not established in the Union, whereby the controller and the processor shall be exempt from that liability, in whole or in part, only if it proves that that member is not responsible for the event giving rise to the damage;

© Published and reproduced with kind permission by Global Legal Group Ltd, London
3 What Should Organisations Consider Before Applying for BCR?

The use of BCR as an appropriate safeguard for international data transfers from the EEA requires the approval of the competent supervisory authority in the relevant jurisdiction following the consistency mechanism set out in Art. 63 and 64 GDPR. The competent supervisory authority will approve the BCR under the condition that:

a) BCR are legally binding and enforceable on the undertakings concerned;
b) BCR expressly confer on the data subjects enforceable rights concerning the processing of their personal data; and
c) BCR comply with the minimum information requirements set out in Art. 47 para. 2 GDPR.

Before applying for BCR approval, an organisation should carefully consider and answer some key questions:

What does the company want to achieve with the approved BCR?

Is the only objective to facilitate the free flow of personal data within the Group? If so, has the organisation considered any alternatives to achieve this objective, such as concluding an intra-group data transfer agreement (“IGDTA”)? Alternatively, is the company’s goal, besides safeguarding cross-border data transfers, also to achieve and demonstrate accountability and commitment to responsible data use? If so, the organisation should assess whether BCR are the right approach or whether there are other options such as certification or a code of conduct, which might be more suitable for achieving the interests of the organisation.

What will be the scope of the BCR?

Will the BCR only cover personal data transferred from the EEA within the Group or will they cover all processing of personal data within the Group? This last option would include any data and go far beyond the legal requirements extending the liability and privacy rights. This extension is ultimately a decision that each organisation must take and may be appropriate for organisations that have decided to establish the same set of rules, standards and rights throughout the whole organisation, irrespective of the jurisdiction and legal requirements. The organisation must also determine if it wants to cover all personal data or limit the BCR to only a set of data such as HR or customer data. Finally, the organisation must determine if all members of the Group shall be bound by the BCR or only a selected number of companies.

Which supervisory authority should be the lead authority for the BCR (“BCR Lead”)?

The BCR Lead is the authority that acts as the single point of contact with the applicant organisation during the authorisation procedure and the application process in its cooperation phase. The BCR Lead may differ from the “one-stop-shop” lead supervisory authority according to Art. 56 GDPR, which is mainly involved in handling data breaches and investigatory or enforcement activities in cross-border processing operations within the EU. The organisation applying for BCR authorisation must justify the reasons why a particular supervisory authority should be considered as the BCR Lead. The criteria for such justification are set out in WP 263:

a) the location of the Group’s European headquarters;
b) the location of the company within the Group with delegated data protection responsibilities;
c) the location of the company which is best placed (in terms of the management function, administrative burden, etc.) to deal with the application and to enforce the BCR in the Group;
d) the place where most decisions in terms of the purposes and the means of the processing (i.e. transfer) take place; and
e) the Member State within the EU from which most or all transfers outside the EEA will take place.

For companies with their head office or principal place of business in the EU, the justification is quite simple. However, how should companies with their registered office outside the EU and without a principal place of business in the EU choose the appropriate supervisory authority and justify their choice? What arguments could be put forward if there is no Member State within the EU from which most or all transfers are made outside the EEA, but such transfers are roughly the same between all entities in the EU? In this case, the organisation may delegate responsibilities to the Group company that is best placed to process the application for BCR on behalf of the Group. This entity should be located in one of the most important countries for the Group with a strong presence and at the same place as the chosen supervisory authority.

Once the organisation has selected the BCR Lead based on the criteria mentioned above, it will submit its application to that supervisory authority. It should be noted, however, that the selected supervisory authority is not obliged to accept the choice if it believes that another

g) how the information on the BCR – in particular, on the provisions relating to the general data protection principles, the rights of the data subjects, and the liability for any breaches of the BCR – is provided to the data subjects;
h) the tasks of any data protection officer designated in accordance with Art. 37 GDPR or any other person or entity in charge of monitoring compliance with the BCR, as well as monitoring training and complaint handling;
i) the complaint procedures;
j) the mechanisms for ensuring verification of compliance with the BCR. Such mechanisms shall include data protection audits and methods for ensuring corrective actions to protect the rights of the data subject. The results of such verification should be communicated to the DPO or any other person in charge of monitoring compliance with the BCR, and to the board of the controlling undertaking, and should be available upon request to the competent supervisory authority;
k) the mechanisms for reporting and recording changes to the BCR and reporting those changes to the supervisory authority;
l) the cooperation mechanisms with the supervisory authority to ensure compliance by any member of the group of undertakings, or group of enterprises engaged in a joint economic activity, in particular by making available to the supervisory authority the results of verifications;
m) the mechanisms for reporting to the competent supervisory authority any legal requirements to which a member of the group of undertakings, or group of enterprises engaged in a joint economic activity, is subject in a third country, which are likely to have substantial adverse effect on the guarantees provided by the BCR; and
n) the appropriate data protection training for personnel having permanent or regular access to personal data.

Which BCR should be implemented?

The organisation must determine if it wants to apply for BCR for controllers or BCR for processors, or both. Depending on that decision, the appropriate requirements must be fulfilled.

What will be the scope of the BCR?

Will the BCR only cover personal data transferred from the EEA within the Group or will they cover all processing of personal data within the Group? This last option would include any data and go far beyond the legal requirements extending the liability and privacy rights. This extension is ultimately a decision that each organisation must take and may be appropriate for organisations that have decided to establish the same set of rules, standards and rights throughout the whole organisation, irrespective of the jurisdiction and legal requirements. The organisation must also determine if it wants to cover all personal data or limit the BCR to only a set of data such as HR or customer data. Finally, the organisation must determine if all members of the Group shall be bound by the BCR or only a selected number of companies.
supervisory authority is more suitable to be the BCR Lead; in particular, taking into account the workload and number of pending BCR applications. The requested supervisory authority will share the application with all concerned supervisory authorities to make a final decision on which supervisory authority is appointed as BCR Lead. It is advisable that the organisation contacts the selected supervisory authority before applying to check whether the supervisory authority is, in principle, willing to act as BCR Lead or whether there may be objections from the supervisory authority; for example, due to lack of resources to deal with the application in a timely manner.

### What should the liability system look like?

Art. 47 para. 2 requires the acceptance by the controller or processor established on the territory of a Member State of liability for any breaches of the BCR by any member concerned not established in the Union. WP 256 and WP 257 provide that, where it is not possible for a Group with particular corporate structures to impose an obligation on a specific entity to take all the responsibility for any breach of the BCR outside of the EU, it may provide that every BCR member exporting data out of the EU on the basis of the BCR will be liable for any breaches of the BCR by the BCR member established outside the EU which received the data from this EU BCR member. Will it be acceptable for the BCR Lead to introduce an alternative liability system in line with the Standard Contractual Clauses? If not, which Group company could take responsibility? What are the options? Clarification on this issue is crucial, especially for companies based outside the EU which do not have their main establishment in the EU. For some organisations, it may not be feasible to allocate responsibility for the payment of damages to a local entity as a result of a breach of the BCR by a Group company outside the EU.

### What is the implementation status of the data privacy management programme within the organisation?

Has the organisation already implemented global standards, policies and procedures, and if so, what is the maturity level at the corporate level and throughout the organisation? Where are potential gaps and risks? Depending on the groundwork done and the maturity level of the data protection management programme, the BCR approval process may take a longer or shorter time.

### Is the buy-in of key stakeholders secured?

Do key stakeholders, from executive management to key country organisations and functions, offer their buy-in to the process? Stakeholder support requires their awareness and understanding of the need and benefits of implementing BCR, the commitments that each business unit and function must make with BCR approval, and the expectations placed in them. Preliminary discussions and a presentation of the business case to these stakeholders are therefore an essential step before applying for BCR.

### Are there sufficient resources and expertise to manage the approval and implementation of BCR?

Is there a team in place to develop the BCR, collect all relevant information, involve the relevant functions, discuss with the BCR Lead and manage the communication and implementation of the BCR across the organisation? This team may consist of a leader and project manager, as well as contributors to critical functions and the most important markets. A properly functioning internal team is crucial to a smooth approval process and implementation throughout the organisation. For smaller companies with fewer resources and expertise in data protection and project management, the involvement of external experts should be considered.

### Why Should Companies Invest in BCR?

The approval of the BCR is an essential step in the whole process. However, the BCR have no practical effect if they are not correctly implemented throughout the Group. Therefore, in parallel to the approval process, it is crucial that the organisation that is responsible for the implementation of the BCR puts in place a concrete and enforceable communication and implementation plan, with responsibilities and reasonable timelines. Here are some suggestions as to what such a plan should contain at the minimum: A communication plan that sets out who should inform whom, how, when and about what, during the whole process. When applying for BCR approval, all Group companies and functions at the corporate and local level should be informed of the content and impact of the BCR, in particular their obligations, and of the progress of the BCR approval process. They should also be informed of the steps they need to take before approval to best prepare for the implementation of the BCR. Throughout the process, it is also advisable to address possible problems, questions and concerns to ensure the broadest possible support and to prevent serious issues or concerns from arising following the approval of the BCR. In some countries, works councils must also be informed or consulted, and finally, once approved and implemented, all employees who regularly process personal data must be informed and trained. Clear roles and responsibilities must be assigned to ensure appropriate communication at each level of the organisation.

An implementation plan that is addressed to those functions and individuals responsible for implementing the privacy management programme and the BCR – in practice, the data protection officers, managers or champions – and outlines what needs to be done, when and how. The steps may include the preparation by adopting the Group privacy policy framework and implementing the data protection management programme at the local level, signing the BCR and making them binding upon employees, training employees, verifying compliance with the BCR and handling complaints. Effective BCR require the establishment of an organisation with responsible persons at corporate and local level to implement the BCR and monitor compliance. A person at corporate level should be appointed to maintain an updated list of BCR members, monitor the state of implementation and any changes, and report annually to the supervisory authority.

### Why Should Organisations Consider once BCR Approval is Obtained?

In practice, many companies have concluded so-called intra-group data transfer agreements (“IGDTA”) covering the cross-border transfer of personal data within their Group. So why should companies go through the effort of implementing BCR when they can achieve the same goal with an IGDTA? Companies with an IGDTA meet the legal requirements for cross-border data transfer. However, they may not benefit from the impact of BCR, which significantly increase awareness and understanding of privacy requirements within the organisation and establish accountability for compliance with data protection requirements in each function and business unit at corporate and local levels throughout the organisation. Also, the...
Organisations that develop and implement BCR regularly aim to achieve an appropriate data protection governance structure with uniform standards and processes across the enterprise, and not only to transfer their data legitimately within the Group. With the approval of the BCR by the supervisory authorities, organisations also want to show that they not only take data protection seriously, but also effectively implement the requirements in the company and assume responsibility for compliance with data protection.

BCR are based on a comprehensive and effective data protection management programme with all the elements required to demonstrate accountability. These elements include:

a) a governance structure with leadership and oversight of the data protection programme;

b) a policy framework with policies and procedures to ensure fair and responsible processing of personal data;

c) transparency through appropriate communication to data subjects;

d) risk assessment and management at the programme and data processing level;

e) awareness raising and training of employees and others who process personal data;

f) monitoring compliance with the data protection programme and verification of its effectiveness through regular self-assessments and internal or external audits; and

g) processes to adequately respond to data subjects’ rights, complaints and inquiries, as well as privacy incidents, and to enforce compliance with internal rules.

Organisations subject to the GDPR and other stringent data protection acts must establish a comprehensive data protection management programme, including all the elements listed above, to ensure compliance with the applicable requirements and responsible data use. With the implementation of such a privacy management programme, organisations are ready to consider applying for BCR approval in order to benefit from a valid data transfer mechanism, while increasing their commitment to privacy within the company and promoting a culture of responsible data use.

To obtain approval of the BCR and ensure compliance with the commitments that are made with the application, the data privacy management programme must, however, include specific procedures and processes. The organisation must assign responsibilities for the implementation of the BCR to each BCR member; in particular, for binding the company and its employees to the BCR and for publishing notices. It must further establish a complaint handling process, develop awareness-raising and training plans and have a mechanism to implement these plans, such as the introduction of regular e-learning for all employees and tailor-made training for specific functions and persons with data protection responsibilities. The organisation must establish an audit framework and a programme to ensure that internal or external accredited auditors regularly verify compliance with the BCR. A mechanism must also be put in place to track all changes and inform BCR members and the supervisory authority. A list of BCR members must be maintained and made available to all members, who are required to inspect that list before transferring personal data across borders.

BCR are ultimately a formalisation and publication of the data protection management programme. At the same time, they are a mechanism for demonstrating accountability to regulators, business partners, customers and individuals and integrating data protection and security into the company’s culture. Processors also gain an immediate competitive advantage compared to other service providers that do not have BCR. The benefits of BCR are apparent and should be considered by any multinational company with cross-border data flows.

6 Conclusions

BCR are not only a sustainable legal basis for data transfer but also a system that enables companies with approved BCR to be transparent to regulators, customers, consumers and business partners by disclosing the company’s policies and procedures on how they process and secure personal data. At the same time, BCR help organisations demonstrate that they take data protection seriously and that they have adopted appropriate data management practices to ensure compliant and responsible data processing throughout the Group. By implementing BCR, organisations affirm their responsibility to comply with legal requirements, and regularly even go beyond, by implementing common standards and rights for individuals across the Group. BCR help to further improve the quality and maturity of the Group’s privacy management programme by fostering a culture of internal compliance and accountability and strengthening the overall trust of individuals, customers, business partners and regulators.

Implementing BCR brings a whole range of benefits not only for the Group itself but also for the data subjects and the supervisory authorities. The effort involved in the approval and implementation process pays off in any case, measured by the advantages for multinational companies, large or small, which stand for the legally compliant and responsible handling of personal data. At the same time, and as further motivation for companies to invest in BCR, it would be desirable for supervisory authorities to formally recognise BCR as an accountability system beyond a data transfer mechanism, along with certifications and codes of conduct, and to find ways to further speed up the approval process.
Daniela Fábián Masoch
FABIAN PRIVACY LEGAL GmbH
Bäumleingasse 10
4051 Basel
Switzerland
Tel: +41 61 544 44 01
Email: daniela.fabian@privacylegal.ch
URL: www.privacylegal.ch

Daniela is the founder and executive director of FABIAN PRIVACY LEGAL, a law firm specialised in international, European and Swiss data protection laws, governance, risk management and programme implementation. Daniela is an attorney at law and Certified Privacy Professional with over 25 years of experience in data protection, labour law, risk and programme management, security and related matters. She advises multinational companies from various industries in the EU, Switzerland and the US on the evaluation, development and implementation of data protection strategies, governance models and global privacy programmes, as well as data transfer mechanisms, with a pragmatic approach. Before commencing her own business in 2015, Daniela held various positions at Novartis, including Global Head of Data Privacy, where she was responsible for setting the Group’s strategic direction for privacy, and for building, implementing and overseeing the global privacy function, global privacy management programme and Group BCR.

FABIAN PRIVACY LEGAL is a boutique law firm specialising in international, EU and Swiss privacy laws and related matters, privacy policies, risk management and programme implementation.

Our strengths are the combination of expert knowledge and practical in-house experience, an excellent network with industry groups and data protection associations, and close cooperation with experts from a variety of related fields, such as cybersecurity and cybercrime, as well as corresponding law firms advising on local legal issues. We approach mandates with a global, solution-oriented and practical approach to deliver pragmatic and sustainable solutions.

Our clients are large and small companies in a wide range of industries, including pharmaceuticals, biotech and medical devices, technology, consumer goods, luxury goods and beverages, transportation and logistics, automotive, insurance, financial institutions and chemicals.
Chapter 4

Initiatives to Boost Data Business in Japan

Anderson Mōri & Tomotsune

I Introduction

In an effort to increase data business in Japan, the government has enacted new legislation and established various supporting guidelines in recent years. In particular, the government issued, and continues to update, guidelines focusing on private businesses utilising big data and artificial intelligence (AI) to clarify and analyse legal issues. In addition, the government issued specialised guidelines for various industries, such as agriculture and gas. Additionally, the government is considering ways to strengthen regulations regarding competition policy. Finally, many private firms intend to start “information bank” platform businesses.

II New Protected Data Category – “Limited Provided Data”

1. Legal protection for data under Japanese law

Data is intangible, and because it is not the subject of rights under the Civil Code, such as ownership or possession, usufruct, or security interest, it is not possible to prescribe the existence or absence of rights pertaining to data based on concepts of ownership or possession (see Article 206 and Article 85 of the Civil Code). As described below in Part III, Concerns over damage caused by leaks and unauthorised use of data

(see Article 206 and Article 85 of the Civil Code). As described below in Part III, Concerns over damage caused by leaks and unauthorised use of data, the cases in which data is subject to legal protection (either as intellectual property, or as a trade secret under the Unfair Trade Practices Act) are limited, so the protection of data is generally achieved through contracts between the interested parties.

Although data can be protected by copyright, patent, and trade secret law, these rights may not adequately protect data for the following reasons.

Works that are subject to protection by copyright are prescribed as productions that express thoughts or sentiments in a creative way (Article 2(1)(i) of the Copyright Act). In many cases, it would be difficult to find a creative element in a collection of data, such as data that is mechanically generated by devices including sensors, cameras, or the usage logs of smartphones, etc.

Also, inventions that are subject to patent protection are highly advanced creations of technical ideas utilising the laws of nature. Cases in which data would be subject to patent protection are limited.

By contrast, data may be subject to legal protection as a trade secret under the Unfair Trade Practices Act if the data embodies know-how of an entity involved in the creation of data or in the distribution or utilisation of data (such as know-how related to production methods in the manufacturing industry, to data cleansing by sensor manufacturers, or to utilisation of data by service development providers), and the data: (i) is managed as a secret; (ii) has utility; and (iii) is not in the public domain. Yet data will not necessarily be protected as a trade secret if it will be distributed during a transaction. The following table provides an outline of intellectual property rights, etc. relating to the protection of data.

<table>
<thead>
<tr>
<th>Type of right</th>
<th>Nature of right</th>
<th>Ability to be used for data protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Copyright</td>
<td>The work must be a production in which thoughts or sentiments are creatively expressed and which falls within the literary, academic, artistic or musical domain (Article 2(1)(i) of the Copyright Act).</td>
<td>The cases in which mechanically generated data can be found to have a creative element are limited.</td>
</tr>
<tr>
<td>Patent</td>
<td>A patent right for a highly advanced creation of technical ideas using the laws of nature that is industrially applicable will become effective upon registration of the invention’s establishment. Patent examination is not available for inventions that do not have novelty or an inventive step (Article 2(1), Article 29(1), and Article 66(1) of the Patent Act).</td>
<td>Regardless of the method of processing or analysing data, the cases in which the data itself can be found to be a highly advanced creation of technical ideas utilising the laws of nature are limited.</td>
</tr>
<tr>
<td>Trade secret</td>
<td>Information is a trade secret if it: (i) is managed as a secret; (ii) has utility; and (iii) is not in the public domain. In the case of a statutorily prescribed act, such as acquiring a trade secret by unfair means (unfair competition), the aggrieved party may seek an injunction, damages, or criminal penalty (Article 2(6), Article 2(1)(iv) through (x), Article 3, Article 4, Article 21, and Article 22).</td>
<td>Data can enjoy legal protection if the elements in (i) through (iii) are satisfied.</td>
</tr>
</tbody>
</table>

2. Protection under the Unfair Competition Prevention Act

As stated above, data that satisfies the three elements contained in Article 2 of the Unfair Competition Prevention Act will enjoy protection as a “trade secret”.

ICLG TO: DATA PROTECTION 2019
© Published and reproduced with kind permission by Global Legal Group Ltd, London
However, because there has been continued innovation in information technology, such as IoT and AI, and the source of companies’ competitive advantage is starting to become data and its utilisation, it is necessary to establish a business environment that enables the safe and reliable utilisation of data. In response to these changes, the government recently enacted the Act to Partially Amend the Unfair Prevention Act, etc. in May 2018 (“Amended Unfair Competition Act”). The Amended Unfair Competition Act introduced remedial measures in civil law, such as injunctions against the unauthorised acquisition or use, etc. of data that is provided in a protected form such as by ID or password, on the basis that this activity constitutes “unfair competition”.

The data that is subject to protection under the Amended Unfair Competition Act is “limited provided data”, which means “technical or business information accumulated or managed in significant volume by electromagnetic means as information provided to certain persons as a business (other than information managed as a secret)” (Article 2(7) of the Amended Unfair Competition Act).

The elements of applicable data and the unfair competition activities that are subject to the new regulations are as follows:

**Elements of data that are the subject of protection**

Data that meets the following elements should be subject to protection:

(i) **Managed with technology**

The data must be managed by appropriate electromagnetic access control means (such as ID and password, dedicated network, data encryption, or scrambling) for provision to only a certain limited scope of persons. Further, there must be a clearly recognised management intention that third parties other than those persons contemplated in the contract with the data provider may not use or be provided with the data.

(ii) **Limited provision to outside parties**

Unlike “trade secrets”, which are managed as a secret and are used in-house by the owner or, as an exception, disclosed to limited persons who have executed a confidentiality agreement, the data must be of a kind that is intended to be optionally provided to certain outside parties in response to their requests.

(iii) **Utility**

The data must be recognised as having commercial value, by stripping the data objects of any illegal or immoral content, and by combining the data objects together.

**Unfair competition activities regarding data**

The following activities would be deemed as “unfair competition activities” and remedial measures would be introduced for these activities:

(i) **“Unauthorised acquisition” type**

Where an unauthorised outside party acquires data through a management breach or, having so acquired the data, uses the data or provides it to a third party (Article 2(1)(x) of the Unfair Competition Prevention Act). In this context, “management breach” means an act that is harmful to the data provider’s management of the data (such as unauthorised access or trespassing), or an act equivalent to fraud, etc. in causing the data provider to provide the data after removing technical management measures (such as acts of fraud, violence, or threat).

(ii) **“Extreme bad faith” type**

Where data, which is subject to a condition that provision to third parties is prohibited, is acquired from a data provider and is used in activity that is equivalent to embezzlement or defalcation (a form of activity that betrays an advanced relationship of trust between parties to a service agreement, etc.) with the purpose of obtaining unjust profit or causing damage to the data provider (a “profit or harm motive”), or where the data is provided to a third party for a profit or harm motive (Article 2(1)(xv) of the Amended Unfair Competition Prevention Act).

(iii) **“Subsequent acquisition” type**

Where a person acquiring data knows that an improper act took place in relation to that data and nevertheless proceeds to acquire that data, or uses the data so acquired or provides it to a third party (Article 2(1)(xii) and (xv) of the Amended Unfair Competition Prevention Act).

Where a person acquiring data did not know at the time of the acquisition that an improper act took place in relation to such data, and, after subsequently becoming aware of such improper act (i.e. acting in bad faith), provides the data to a third party (Article 2(1)(xiii) and (xvi)). Cases where the data is provided within an authorised scope prescribed in a transaction that predates the subsequent acquirer’s bad faith action are excluded.

---

**III Guidelines Focusing on Big Data**

The government’s Guidelines focus on matters that should be included in data contracts, meaning contracts relating to the utilisation, processing, transfer, and other handling of data. The Guidelines have a view towards promoting reasonable negotiations and execution of contracts, reducing transaction costs and diffusing data contracts, etc. in light of the fact that data contracts tend to be incomplete contracts that fail to cover any events that may occur after the execution thereof. The basic ideas are as follows:

1. **Purpose**

Because data contracts have not been broadly executed in general and contractual practices have not become standardised, data contracts are likely to cause various problems when they are executed in the future. The Guidelines aim to, with respect to data contracts that have the characteristics described above and for which no standard form is established, reduce transaction costs and diffuse data contracts in order to promote the effective use of data. The Guidelines accomplish these goals by presenting major issues and questions for each type of contract and by providing examples of contractual terms that are easily accessible to the public and factors to be considered when preparing those terms.

The Ministry of Economy, Trade and Industry and other authorities have already published two guidelines related to data contracts. First, the “Contract Guidelines for Promotion of Data Transaction”, published in October 2015, presented the conditions, points and other matters relating to the provision of data by rights holders of the data, on the assumption that the rights holders can be clearly identified from among the interested parties. Second, the “Contract Guidelines on Data Utilization Rights ver. 1.0”, published in May 2017, presented the consultation process for determining the holders of utilisation rights and the process for determining the contractual utilisation rights.

However, the two guidelines above were not intended to comprehensively present the types and terms of all data contracts. Further, it is apparent from the rapid progress of AI and IoT technologies in recent years that the environment surrounding data contracts has evolved dramatically on a daily basis against the background of technological innovation that enables collection, processing and analysis of enormous amounts of data. Therefore, the practice of drafting data contracts and the guidelines for the discipline of that practice must also respond to those drastic changes.

Typical examples of the difficulties in this area are: (1) issues related to so-called data ownership; (2) issues of how to
Importance and issues of data distribution and utilisation

Recently, the amount of data related to transactions has explosively increased in connection with the promotion of, among other things, IT adoption in those transactions. In some cases, data creates added value when combined with other data, and the combination of multiple data across industries is especially expected to lead to open innovation. To enhance the added value of data and to strengthen competitiveness, it is important to expand the subjects and types of data to be used and to utilise that data in various combinations.

1) Promotion of data utilisation

In many cases, data itself is not valuable, and value is created only after processing and analysing data and developing methods for utilising the data for business activities. Therefore, it would be desirable, when conducting contractual negotiations, to empower the parties that have the method or ability to utilise the data, encourage those parties to utilise the data, and distribute profits gained from the data utilisation among the parties.

Certain types of data create sufficient value only when collected in a certain amount. For example, real-time driving data of vehicles can be used for congestion analysis when the data of a large number of vehicles are collected, and that data creates value that cannot be realised simply by analysing the data of each vehicle. Similarly, in the case of data regarding the operation status of machine tools, etc., it becomes possible to perform statistically meaningful analysis on the operation of those tools only by accumulating data of a large number of tools. In these types of cases, the party that can collect and utilise the large volume of data should be authorised to use the data.

In connection with allocation of the utilisation rights, it is also important that the resulting interests are distributed among the parties in an appropriate manner. In order to collect, process, and analyse data and develop utilisation methods, etc., parties must make hardware investments, such as sensors and servers, as well as human investments, such as data analysts. It is desirable to provide incentives for these investments and to grant the parties making those investments appropriate profits (returns).

2) Concerns over damage caused by leaks and unauthorised use of data

There are certain risks in the distribution and utilisation of data. In general terms, data can be easily duplicated and, if there is no appropriate management system, may be leaked to the outside through unauthorised access. Therefore, when data contains a company’s confidential information, the company may be anxious that the trade secret and know-how might be leaked out of the company through the provision of the data. Moreover, if any personal information is included in the data, not only may the industry competitiveness of the parties be diminished, but privacy rights may also be infringed.

In considering data distribution and utilisation in individual cases, it is essential to pay careful attention to the concerns about these risks. The risks may be minimised through appropriate contractual and technical measures, so the parties should understand those various measures correctly evaluate the risks and benefits and to execute reasonable data contracts. The methods for preventing any leaks or unauthorised utilisation of trade secrets and know-how, etc. are described in section II above.

3) Increased complexity and sophistication of contracts and significance of these Guidelines

If the parties to data contracts, which are a new type of contract for which the matters to be decided are becoming increasingly complex and sophisticated, can build reasonable business relationships for data distribution and utilisation at a low cost, the competitiveness of the parties as well as national competitiveness would increase, in combination with the application of laws, including the Antimonopoly Act and the Unfair Competition Prevention Act.

However, in light of the principle of freedom of contract, matters such as the selection of counterparty, determination of contents, and method of contracting are left to the choice of the contracting parties. Therefore, these Guidelines only indicate the matters to be set forth in contracts and do not, as a matter of course, restrict any freedom of contract.

Specifically, for the purpose of generally diffusing data contracts among various transactions, these Guidelines introduce matters to be included in contracts executed between business operators for the distribution, utilisation, sharing, etc. of data.

In order to increase the sophistication of contracts, it is necessary to remember that utilisation rights can be freely stipulated by contract. Since data is intangible by nature and is not subject to ownership, the utilisation rights can be freely determined between the parties by contract. Therefore, to increase the sophistication of data contracts, the parties should flexibly determine the conditions of use and should set forth specific details of the utilisation rights and other matters, with reference to these Guidelines and taking into consideration the degree of contribution to the creation and utilisation of data and other factors.

4) Promotion of innovation

These Guidelines aim to support parties who wish to distribute and utilise data, and to enable the utilisation of new, undiscovered value by not only promoting traditional innovations in which data is utilised through the efforts of individual companies without opening the data, but also by further expanding the possibilities of open innovation.

Another purpose of these Guidelines is to encourage the utilisation of data and promote open innovation by providing the concept of data contracts and contract terms, etc. and by giving consideration to various positions.

IV Competition Policy Focusing on Big Data and Platform Business

Potential problems under the Act on Prohibition of Private Monopolization and Maintenance of Fair Trade (the “Antimonopoly Act”) can emerge in cases where unilateral contract provisions, etc. are imposed against a backdrop of what amounts to a position of dominance in the negotiation of contracts between large corporations on the one hand, and medium-sized, small, and venture corporations on the other hand, or in cases where the parties conduct exclusive dealing and restrictive trading, etc.
1. Abuse of a dominant bargaining position

Abuse of a dominant bargaining position under the Antimonopoly Act (Article 2(9)(v)) can become a problem if there is a relationship of relative dominance between contracting parties. In this regard, the “Guidelines Concerning Abuse of a Dominant Bargaining Position in Service Transactions under the Antimonopoly Act”, published by the Japan Fair Trade Commission, state the following views:

(i) In a service transaction, a service provider can suffer undue disadvantage if a service delegator with a dominant bargaining position abuses its superior bargaining position by unilaterally causing a service provider to assign (including through licensing) the service provider’s rights in deliverables to the service delegator, or by restricting the use of deliverables, technologies, etc. for other purposes (i.e., secondary use) to an extent not contrary to the purpose of the service transaction, on the basis that the deliverables, etc. have been obtained in the course of the service transaction with the service delegator or have been created at the expense of the service delegator.

(ii) Even under those circumstances, however, abuse of a dominant bargaining position does not arise if consideration for assignment of the rights pertaining to, or for restriction on secondary use of, Derivative Products is paid separately, or if negotiations for consideration are conducted in a manner that includes consideration for the assignment or restriction.

(iii) By contrast, abuse of a dominant bargaining position does arise in service transactions that are unreasonably disadvantageous to the service provider, such as cases where consideration for the assignment, etc. of the rights pertaining to Derivative Products is unreasonably low or where the assignment, etc. of the rights pertaining to Derivative Products is essentially forced. Accordingly, in contracts regarding the development of AI-based software between Vendors and Users where the terms and conditions are basically entrusted to the independent judgment of each party, abuse of a dominant bargaining position can occur if either party exploits a dominant bargaining position over the other party unjustly in light of ordinary business practices in order to delay the payment of the price, to reduce the price, to conduct a transaction or do-over for significantly lower consideration, or to unilaterally handle rights, etc. pertaining to raw data, a training dataset, a training program, or a trained model for the use of AI technology (e.g., assignment of such rights and restriction on secondary use). However, abuse of a dominant bargaining position does not emerge in cases where appropriate consideration is paid separately for the assignment of rights or restriction on secondary use, or where negotiations for consideration are conducted in an appropriate manner that includes the consideration for the assignment or restriction, including conditions for income sharing in secondary use.

2. Exclusive dealing and restrictive trading, etc.

Unfair trade practices under Article 19 of the Antimonopoly Act, such as exclusive dealing and restrictive trading, can occur when parties establish terms of use for AI-based software and stipulate contractual provisions for restriction on the use of such software in contracts regarding AI-based software.

In a licensing contract, the following act is, in principle, deemed to constitute an unfair trade practice: imposing an obligation to vest in the licensor or a business operator designated by the licensor the rights in improved technology developed by the licensee, or the obligation to grant an exclusive license to the licensor with respect to that improved technology. Even if the rights or licensing were shared, that act would be considered an unfair trade practice if the act constituted an impediment to fair competition (12) of the Designation of Unfair Trade Practices (Fair Trade Commission Public Notice No. 15 of 1982)).

By contrast, imposing an obligation to license the licensee’s improved technology in a non-exclusive manner to the licensor does not, in principle, constitute an unfair trade practice if the licensor has the discretion to use the improved technology developed by the licensee. In addition, if the improved technology developed by the licensee cannot be used without the technology licensed by the licensor, it is generally understood that the act of imposing an obligation to assign the rights pertaining to the improved technology to the licensor for reasonable consideration does not constitute an impediment to fair competition. Furthermore, the act of imposing an obligation to report to the licensor any knowledge or experience obtained in the course of using the licensed technology does not, in principle, constitute an unfair trade practice unless, in effect, that obligation requires the licensee to license the know-how acquired by it to the licensor.

3. Platform business regulation

The Japanese government intends to introduce new regulations regarding the platform business industry, including IT global giants. These new regulations are subject to ongoing discussions and might include introduction of data portability systems and of focused regulations related to outsourcing. Outsourcing the creation of programs is considered to be an “information-based product creation contract” under the Act against Delay in Payment of Subcontract Proceeds, Etc. to Subcontractors (the “Subcontractors Act”). Under the Subcontractors Act, a business operator that places an order (the main subcontracting entrepreneur) is prohibited from delaying payment, reducing subcontract proceeds, and engaging in transactions, etc. for significantly low subcontract proceeds.

V Information Bank

The so-called “information bank” platform would start in 2019. In this new business model, an information bank collects and stores data relating to personal consumers and, based on their consent to the data being shared, the information bank would provide the personal information to businesses in exchange for a fee. The platform could be run by a system development company or a telecommunications provider, for example.

The information bank could hold several types of data, including social network profiles, fitness data tracked through wearable devices, online shopping histories and GPS locations. Individuals would be able to choose the information that they are willing to share, and with whom.

Businesses would be able to gain access to information from other companies and industries, in addition to customer data that they collected on their own. This access will allow businesses to create products and services that are better suited to customers’ interests.
Takashi Nakazaki
Anderson Mōri & Tomotsune
Otemachi Park Building
1-1-1 Otemachi
Chiyoda-ku
Tokyo 100-8136
Japan
Tel: +81 3 6775 1086
Email: takashi.nakazaki@amt-law.com
URL: www.amt-law.com

Takashi Nakazaki is special counsel at Anderson Mōri & Tomotsune with broad experience in the areas of data protection and privacy (including big data and IoT), information security, intellectual property, licensing, and payment services including cryptocurrency. Further, he has experience working on matters relating to cyber law issues such as cloud computing, domain names, e-commerce, social media and other technology-related areas, telecommunications, labour and general corporate law.

In the area of data protection law, he frequently advises various international and domestic online service companies including operators of online games, online gambling and SNS. In addition, he regularly assists the Japanese government in data protection and cyber law areas including “National Omote-nashi project” and “AI & Data Contracts Guidelines” and continuously leads IAPP Tokyo as a co-chair.

Mr. Nakazaki has been ranked as one of the top lawyers in the data protection and information security field for the last several years.

Anderson Mōri & Tomotsune is a full-service law firm formed by the merger and consolidation of the practices of three leading Japanese law firms: Anderson Mōri, which established its reputation as one of the largest and most established international law firms in Japan since its inception in the early 1950s; Tomotsune & Kimura, particularly known for its expertise in international finance transactions; and Bingham Sakai Mimura Aizawa, a premier international insolvency/restructuring and crisis-management firm.

With a long tradition of serving the international business and legal communities, our superior expertise, coupled with our standing as one of the largest law firms in Japan, translates to not only high-quality services but also time and cost efficiencies, which we share with our clients.
1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

The principal legislation is as follows:

- Law no. 9887, dated 10.03.2008 “On personal data protection” (“the Law”) as amended.
- Decision of the Parliament no. 211, dated 11.09.2008 “On the appointment of the Commissioner for the protection of personal data”.
- Decision of the Parliament no. 225, dated 13.11.2008 “On approving of the structure, staff and classification of the working positions in the office of the Commissioner for the protection of personal data”.
- Decision of the Commissioner for the protection of personal data no. 8, dated 31.10.2016 “On the countries with an adequate level of protection for personal data” as amended.
- Decision of the Commissioner for the protection of personal data no. 4, dated 27.12.2012 “On exceptions to the obligation to notify the processing of personal data”.
- Decision of the Commissioner for the protection of personal data no. 2, dated 10.03.2010 “On determination of procedures for registration administration of data and their recording, procession and extraction” as amended.

1.2 Is there any other general legislation that impacts data protection?

The Republic of Albania has also ratified the following international acts:

- Convention on the Protection of Individuals regarding the automatic processing of personal data (Law no. 9288/2004, as amended) (“the Convention”).
- Additional Protocol to the Convention regarding supervisory authorities and trans-border flows of personal data (Law no. 9287/2004).

1.3 Is there any sector-specific legislation that impacts data protection?

The competent authority on personal data protection, with the purpose of further regulating the processing of personal data and ensuring the correct implementation of the Law’s provisions, has issued several instructions, guidelines and orders.

1.4 What authority(ies) are responsible for data protection?

The competent authority is the Information and Data Protection Commissioner (“the Commissioner”).

2 Definitions

2.1 Please provide the key definitions used in the relevant legislation:

- “Personal Data”
  “Personal Data” refers to any information relating to an identified or identifiable natural person, directly or indirectly; in particular, by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.
- “Processing”
  “Processing” of personal data means any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, transmission, dissemination or otherwise making available, alignment or combination, photographing, reflection, entering, filling in, selection, blocking, erasure or destruction, even though they are not recorded in a database.
- “Controller”
  “Controller” means the natural or legal person, public authority, agency or any other body which, alone or jointly with others, determines the purposes and means of processing of personal data, in compliance with the laws and applicable secondary legislation, and is responsible for the fulfilment of obligations defined by the Law’s provisions.
- “Processor”
  “Processor” means a natural or legal person, public authority, agency or other body, which processes personal data on behalf of the controller.
- “Data Subject”
  “Data Subject” means any natural person whose personal data are being processed.
- “Sensitive Personal Data”
  “Sensitive Personal Data” means any information related to the natural person with reference to his racial or ethnic origin, political opinions, trade union membership, religious or philosophical beliefs, criminal record, as well as data concerning his health and sexual life.
3 Territorial Scope

3.1 Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to those laws?

The Law applies, inter alia, to controllers who are not situated in the Republic of Albania, but exercise their activity using any means situated in such territory. In this case, the controller should designate a representative situated in the Republic of Albania.

4 Key Principles

4.1 What are the key principles that apply to the processing of personal data?

- **Transparency**
  The transparency principle is not expressly provided in the applicable legislation, although the same can be carved out by reading the other Law provisions, such as the duty to inform the data subject, processing for a specific purpose and limited in time, etc.

- **Lawful basis for processing**
  Pursuant to the Law, one of the guiding principles is the fair and lawful processing of personal data.

- **Purpose limitation**
  Furthermore, the legislator stipulates that personal data are collected for specific, clearly defined and legitimate purposes and shall be processed in a way that is compatible with these purposes.

- **Data minimisation**
  The principle of data minimisation is not addressed separately in the Law but is applied as a combination of the principles of proportionality and retention.

- **Proportionality**
  Based on the Law provisions, personal data must be proportionate and correlated with the scope of processing, and not excessive in relation to the purposes for which they are collected and processed.

- **Retention**
  The legislator provides that personal data cannot be kept for longer than is necessary for the purpose for which they were collected or further processed. The Law does not contain a specific provision determining the minimum or maximum time for the retention of personal data. However, there exist time limits applicable to specific sectors, as determined by the decision of the Commissioner.

- **Other key definitions – please specify (e.g., “Pseudonymous Data”, “Direct Personal Data”, “Indirect Personal Data”)**
  “Anonymous Data” means any data which, in its origin or during its processing, may not be associated with any identified or identifiable individual.

5 Individual Rights

5.1 What are the key rights that individuals have in relation to the processing of their personal data?

- **Right to access to data/copies of data**
  The data subject shall have the right to obtain, free of charge, from the controller upon written request: a) confirmation as to whether or not personal data concerning him or her are being processed, information on the purposes of processing, the categories of processed data concerned and the recipients or categories of recipients to whom personal data are disclosed; b) communication to him/her, in a comprehensible form, of the data undergoing processing and of any available information as to their source; and c) in the case of automated decisions, information about the logic applied in the decision-making.

- **Right to rectification of errors**
  The data subject has the right to request rectification or deletion of his data, free of charge, whenever he/she becomes aware that data relating to him/her are irregular, false, and incomplete, or have been processed in violation of the Law provisions.

- **Right to object to processing**
  The data subject has the right to object, at any time, free of charge, to the processing of data related to him/her carried out by the controller: i) in the ambit of the performance of a legal task of public interest or in exercise of powers of the controller or of a third party to whom the data are disclosed; or ii) in cases where the processing is necessary for the protection of the legitimate rights and interests of the controller, the recipient or any other interested party unless otherwise provided by the Law.

- **Right to restrict processing**
  The Law does not specifically address this matter. However, controllers are bound to address any request of the data subject regarding the processing of their personal data, especially with regard to data accuracy, further processing, processing purpose, etc.

- **Right to data portability**
  The Law does not address this matter. However, this might apply based on the aforementioned entitlements of the data subject.

- **Right to withdraw consent**
  The data subject has the right to withdraw his/her consent, at any time.

- **Right to object to marketing**
  The data subject has the right to demand the controller not to start processing, or if processing has started, to stop processing of personal data related to him/her for the purposes of direct marketing, and to be informed in advance before personal data are disclosed for the first time and for such a purpose.
6 Registration Formalities and Prior Approval

6.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?

Controllers should notify the Commissioner in advance of any processing of personal data. To this end, the Law provides that controllers, before starting the processing, should notify the Commissioner of the intended activity and categories of personal data, and any changes to the status of notification. The notification to the Commissioner should also contain the intention of the controller to undertake the transferring of personal data to third countries. Deviation from the rule is made where personal data are processed by non-profit organisations of political, religious, or philosophical character, trade unions, etc., and the process refers to their members, sponsors, etc.

The notification form can be filled in and filed online with the Commissioner or printed, filled in and delivered in person to the Commissioner’s office. The notification contains information on the data controller and processor, categories of individuals and data to be processed, purpose of the processing, information on whether an international transfer to third countries will occur, measures adopted to secure the data (i.e., policy and/or regulation documents can be enclosed with the notification form), etc.

The administrative sanctions provided by the Law are applicable by the Commissioner and consist of fines that vary from a minimum of ALL 10,000 up to a maximum of ALL 500,000.

The aforementioned fines apply to natural persons double in cases where the violations are attributed to legal persons. The maximum fine also doubles in the case of processing of personal data without the prior authorisation of the Commissioner.

6.2 If such registration/notification is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?

The notification should contain, inter alia, the following information:

- name and address of the controller;
- purpose of the processing;
- data subject and personal data categories;
- recipients or categories of recipients of personal data;
- proposal for any international transfer that the controller intends to do; and
- general description of measures adopted to secure personal data.

6.3 On what basis are registrations/notifications made (e.g., per legal entity, per processing purpose, per data category, per system or database)?

The notification is performed by the controller, being the same defined by the Law as the natural or legal person, public authority, agency or any other body which, alone or jointly with others, determines the purposes and means of processing of personal data, in compliance with the laws and applicable secondary legislation, and is responsible for the fulfilment of obligations defined by the Law.

6.4 Who must register with/notify the data protection authority (e.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation)?

The obligation to notify the Commissioner applies to all data controllers and processors situated in Albania, as well as those situated outside Albania that exercise their activity using any means situated in such territory (as indicated in our answer to question 3.1 above).

6.5 What information must be included in the registration/notice (e.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes)?

The notification needs to be renewed should changes occur to the information provided to the Commissioner.

6.6 What are the sanctions for failure to register/notify where required?

Notification to the Commissioner is free of charge.

6.7 What is the fee per registration/notification (if applicable)?

The notification needs to be renewed should changes occur to the information provided to the Commissioner.

6.8 How frequently must registrations/notifications be renewed (if applicable)?

Authorisation by the Commissioner is required for the processing of sensitive data for an important public interest and under adequate safeguards. Additionally, prior approval is required in the ambit of the international data transfer to countries without an adequate level of protection for personal data. However, in the latter case, prior approval is not required when:

a) it is authorised by international acts ratified by the Republic of Albania, which are directly applicable;

b) the data subject has given his/her consent for the international transfer;
the transfer is necessary for the performance of a contract between the data subject and the controller or for the implementation of pre-contractual measures addressing the data subject’s request, or the transfer is necessary for the conclusion or performance of a contract between the controller and a third party, in the interest of the data subject;

d) it is necessary for protecting vital interests of the data subject;

e) it is necessary or constitutes a legal requirement over an important public interest or for exercising and protecting a legal right; and

f) transfer is done from a register that is open for consultation and provides information to the general public.

6.10 Can the registration/notification be completed online?

In practice, the registration/notification is delivered in hard copy to the Commissioner’s office.

6.11 Is there a publicly available list of completed registrations/notifications?

On the website of the Commissioner, any interested party might access the electronic registry of the controllers/processors, by inserting their name and business identification number.

6.12 How long does a typical registration/notification process take?

The Law does not set a maximum or a minimum term for the process of notification.

7 Appointment of a Data Protection Officer

7.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.

Based on the Instruction of the Commissioner no. 47, dated 14.09.2018 “On determination of rules on the safety of personal data processed by large data controllers”, large processing data entities, which are considered those controllers or processors which process data by automatic or manual means, by employing six or more persons, directly or by virtue of the processors, are required to appoint a Data Protection Officer (“DPO”), defined as “Contact Person” in the Law.

7.2 What are the sanctions for failing to appoint a Data Protection Officer where required?

Failure to appoint a DPO is sanctioned by fines ranging from a minimum of ALL 10,000 up to a maximum of ALL 1,000,000. The aforementioned fines, applying to natural persons, double in cases where the violations are attributed to legal persons.

7.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect of his or her role as a Data Protection Officer?

The Law is silent on this matter.

7.4 Can a business appoint a single Data Protection Officer to cover multiple entities?

The Law does not specifically address this matter. However, our understanding is that a DPO might be appointed for the purpose of covering multiple entities.

7.5 Please describe any specific qualifications for the Data Protection Officer required by law.

Based on the above-indicated Instruction, the Contact Person should:

a) have full legal capacity to act;

b) have integrity;

c) possess a Bachelor’s degree in law or computer science;

d) have professional skills and ethics;

e) have at least five years of work experience as a jurist or IT expert, or more than three years of work experience at the Commissioner’s office in the capacity of jurist or IT expert; and

f) not have been convicted of any criminal offence.

7.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?

The Contact Person:

a) is responsible for the internal surveillance of fulfilment by the processing entity of the obligations for the protection of personal data;

b) advises the responsible persons on personal data protection;

c) is responsible for the implementation of technical, organisational measures in relation to the personnel and oversees their practical implementation;

d) in the case of engagement of a processor, is responsible for the internal surveillance of its activity, the content and preparation of the contract with the processor. During the implementation period of the contract or authorisation, the Contact Person will verify the fulfilment of the agreed terms and conditions including the engagement or changes of processors, if any;

e) is responsible for the internal surveillance of the international personal data transfer;

f) is responsible for the handover of the documentation on the archiving systems for special registration, for announcing changes and de-registration from the special register in the archiving systems, and for keeping data on the archiving systems which are not subject to registration and making them available to any person which, by law, has the right to access them;

g) is responsible for necessary collaboration with the Commissioner as necessary; and

h) upon request of the Commissioner, is obliged to submit the written authorisation by means of which he or she operates, as well as proof of the skills gained during the professional training.

7.7 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?

The Contact Person(s) should be notified to the Commissioner. In the case of the replacement of the Contact Person, the Commissioner should be notified within 14 days from the date of the replacement.
7.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?

The Law is silent on this matter.

8 Appointment of Processors

8.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?

Pursuant to Instruction no. 19, dated 03.08.2012 “On regulation of the relationship between the controller and processors in case of delegation of processing personal data and the use of a standard contract in cases of such delegation” as amended, the business that appoints a processor to process personal data on its behalf is required to enter into an outsourcing agreement with the processor. In such case, the said instruction also provides for a standard contract template that might be used by the parties for the purpose of delegation of personal data processing.

8.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?

Pursuant to the abovementioned instruction, the outsourcing contract should be concluded in writing and signed by both parties. In addition, the said contract should contain, inter alia, provisions on rules for personal data processing according to the Albanian legislation, measures to be taken by the processor to ensure sufficient data protection, and steps to be taken in case of data breaches.

9 Marketing

9.1 Please describe any legislative restrictions on the sending of electronic direct marketing (e.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?).

By the letter of the Law, collection of personal data for direct marketing purposes requires the explicit consent of the data subject. The concept and rules applicable to direct marketing are further developed by the Commissioner, inter alia, in: Instruction no.16, dated 26.12.2011 “On protection of personal data in the direct marketing and the safety measures” as amended; Instruction no. 6, dated 28.05.2010 “On correct use of SMS for promotional, advertising, information, direct sales, by means of mobile telephony”; and Instruction no. 14, dated 22.12.2011 “On processing, protection and safety of personal data in the public electronic communication sector”.

9.2 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.).

Please refer to our answer to question 9.1.

9.3 Do the restrictions noted above apply to marketing sent from other jurisdictions?

As mentioned in our answer to question 3.1 above, the provisions of the Law apply also to those who are not situated in the Republic of Albania, but exercise their activity using any means situated in such territory. In this case, the controller should designate a representative situated in the Republic of Albania.

9.4 Is/are the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?

The Commissioner is active in promoting and raising awareness of the obligations and rights attached to both controllers and data subjects. Based on information publicly available on the website of the Commissioner, different controllers have received recommendations and/or were subject to decisions (administrative sanctions) of the Commissioner.

9.5 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?

According to Instruction no. 6, dated 28.05.2010 “On correct use of SMS for promotional, advertising, information, direct sales, by means of mobile telephony”, the provision on marketing lists to third parties requires the prior consent of the data subject.

9.6 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?

Generally, the applicable fines range from a minimum of ALL 10,000 up to a maximum of ALL 500,000.

10 Cookies

10.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).

The applicable legislation does not address the matter.

10.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?

This is not applicable.

10.3 To date, has/have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?

This is not applicable.

10.4 What are the maximum penalties for breaches of applicable cookie restrictions?

This is not applicable.
11 Restrictions on International Data Transfers

11.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.

International transfer of personal data to third countries not having an adequate level of protection might be undertaken upon prior authorisation of the Commissioner. In cases where the Commissioner, after assessing the situation, permits the international transfer of personal data to a third country lacking in adequate levels of protection, a set of proper safety measures shall apply. The Commissioner might exempt controllers from requiring authorisation for special categories of personal data. The categories of data falling under the said exemption shall be determined by the Commissioner.

However, the Law provides for exceptions to the obtaining of the prior authorisation in cases of international transfer to a third country having an inadequate level of protection, which are:
- Made based on international treaties ratified by the Republic of Albania, which are directly applicable.
- Consented to by the data subject.
- Necessary for the implementation of the contract between the data subject and controller or for the implementation of the pre-contractual measures, in response to the request of the data subject, or the transfer is necessary for the fulfilment or implementation of the contract between the controller and a third party, in the interest of the data subject.
- Necessary for the vital interest of the data subject.
- Done through a register open to consultation, which provides information to the public in general.
- Necessary or legally required by an important public interest or for exercise/defence of a legal right.

11.2 Please describe the mechanisms businesses typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).

Based on the Law’s provisions, for cases falling outside the above exceptions, companies are required to obtain prior authorisation of the Commissioner.

11.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.

Based on the applicable legislation, international transfers of personal data in countries deemed to have an adequate level of protection are not restricted if the Commissioner has been duly notified. The Decision of the Commissioner for the protection of personal data no. 8, dated 31.10.2016 “On the countries with adequate level of protection for personal data”, provides that countries with an adequate level of protection for international transfers of personal data are, namely, EU Member States and countries that are part of the European Economic Area, members of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data and the related Protocol, as well as countries designated by a decision of the EU Commission.

As for the international transfer of data to countries deemed not to have adequate protection, the prior authorisation of the Commissioner is required, provided that none of the requirements indicated in question 11.1 are met.

In addition to the fact that the letter of law is clear in this respect, the Commissioner’s standpoint is that any international transfer to third countries having an inadequate level of protection must be authorised.

12 Whistle-blower Hotlines

12.1 What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?

The rules on whistleblowing are laid down under the provisions of the Law no. 60/61 “On whistleblowing and protection of whistleblowers”. This law applies to the reporting of, inter alia, alleged corruption practices in public and private sector. The persons entitled to submit whistleblowing reports are individuals that apply for a job position at, or are current or former employees of, the private organisation. Persons whom a report may concern are those who are the subject of this report (i.e. officials of the private organisation and/or public officials).

12.2 Is anonymous reporting prohibited, strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do businesses typically address this issue?

According to the law on whistleblowing, the whistleblower might choose to file anonymous reporting, provided that he/she has clearly and reasonably presented the reasons of anonymity and the reported data are sufficient for the purpose of administrative investigation of the reported case.

13 CCTV

13.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?

The use of CCTV is subject to notification with the Commissioner, with exceptions in cases of processing of personal data which, based on the applicable legislation, has the sole purpose of keeping records for the provision of information to the public in general. Also exempted from the notification are personal data processed for the purpose of protection of the constitutional institutions, national security interests, foreign policy, economic or financial interests of the state, or for prevention or prosecution of criminal offences.

13.2 Are there limits on the purposes for which CCTV data may be used?

Pursuant to Decision of the Commissioner no. 3 dated 05.03.2010 “On processing personal data with video surveillance in buildings and other environments” as amended, the use of the CCTV shall be considered lawful and in accordance with the applicable legislation when it is is used.
1. in the fulfilment of a task defined by a special law;
2. with the consent of the data subject; this is considered possible, in practice, only in restricted cases when the identification of a group of persons inside the camera zone is can be clearly made; or
3. without the consent of the data subject, but always respecting the criteria set out in article 6 of the Law.

In addition, the CCTV can be used only when, inter alia, the purposes of processing the data cannot be accomplished using another system. Moreover, the purposes of the recording should be clearly defined and not exceed the maximum term allowed.

14 Employee Monitoring

14.1 What types of employee monitoring are permitted (if any), and in what circumstances?

The applicable legislation stipulates that the use of video surveillance is allowed only for security reasons. Under no circumstances should video surveillance be used to monitor private areas such as lavatories, changing rooms, etc.

14.2 Is consent or notice required? Describe how employers typically obtain consent or provide notice.

Video surveillance should be carried out in accordance with the requirements set by the applicable legislation. Additionally, the video surveillance process should be duly notified by the employer by affixing notices in the workplace.

14.3 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?

The applicable legislation does not explicitly address the matter; however, the Commissioner, through Instruction no. 11 dated 08.09.2011 “On processing personal data in the private sector” as amended, provides that in cases where, due to the size and organisational structure of the enterprise, it is not possible for employees to exercise personally their rights as stipulated by the Law, the latter can appoint a representative vested with the respective powers.

15 Data Security and Data Breach

15.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?

Pursuant to article 27 of the Law, the controller or the processor is obliged to take appropriate organisational and technical measures for protecting personal data from accidental or unlawful destruction, loss, or unauthorised disclosure/access to personal data transmitted, especially when the processing of data takes place in a network; as well as from any other unlawful form of processing.

15.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

Although there is no specific duty to report data breaches, the legislator sanctions the unauthorised disclosure of confidential information. The Law provides for a fine ranging from ALL 10,000 up to ALL 150,000. Moreover, in some specific cases, a confidential information breach may constitute a criminal offence punishable by a fine or imprisonment of up to two years.

15.3 Is there a legal requirement to report data breaches to affected data subjects? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

Please see the answer above.

15.4 What are the maximum penalties for data security breaches?

Please refer to the answer to question 12.2.

16 Enforcement and Sanctions

16.1 Describe the enforcement powers of the data protection authority(ies).

<table>
<thead>
<tr>
<th>Investigatory Power</th>
<th>Civil/Administrative Sanction</th>
<th>Criminal Sanction</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Commissioner may start investigations on an ex officio or ex parte basis in order to verify compliance with the Law’s provisions.</td>
<td>Pecuniary sanctions vary from a minimum of ALL 10,000 up to a maximum of ALL 1,000,000.</td>
<td>Not applicable.</td>
</tr>
<tr>
<td>State Prosecutor.</td>
<td>Not applicable.</td>
<td>Fine or imprisonment for up to two years (article 123 of the Criminal Code of the Republic of Albania as amended).</td>
</tr>
</tbody>
</table>

16.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?

The Commissioner is entitled to order the blocking, erasure, destruction or suspension of the unlawful processing of personal data.

16.3 Describe the data protection authority’s approach to exercising those powers, with examples of recent cases.

During the investigation process, the Commissioner issues
recommendations, orders that must be complied with, and administrative sanctions, should controllers and processors fail to meet/comply with the Law’s provisions. According to data obtained from the official website, during 2018 the Commissioner issued 29 recommendations, one order and 30 administrative sanctions. The State Prosecutor may start an investigation upon ex parte or Commissioner’s referral of any criminal contravention committed.

16.4 Does the data protection authority ever exercise its powers against businesses established in other jurisdictions? If so, how is this enforced?

We do not have any information in this regard.

17 E-discovery / Disclosure to Foreign Law Enforcement Agencies

17.1 How do businesses typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?

This is not applicable.

17.2 What guidance has/have the data protection authority(ies) issued?

This is not applicable.

18 Trends and Developments

18.1 What enforcement trends have emerged during the previous 12 months? Describe any relevant case law.

As indicated above, during the last year, the Commissioner has been very proactive in issuing various recommendations and administrative sanctions to controllers and processors.

18.2 What “hot topics” are currently a focus for the data protection regulator?

One upcoming development which is worthy of note is the transposition of the EU General Data Protection Regulation (GDPR). To the best of our knowledge, this is expected to take place by 2020.
Chapter 6

Australia

Nyman Gibson Miralis

1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

The Privacy Act 1988 (Cth) (‘Privacy Act’), including the Australian Privacy Principles (‘APPs’).

1.2 Is there any other general legislation that impacts data protection?

The Do Not Call Register Act 2006 (Cth) (‘DNCRA’) and Spam Act 2003 (Cth) (‘Spam Act’) set out limits to direct marketing activities. At the state and territory level, there is much legislation concerned with data protection including, for example: the Information Privacy Act 2014 (ACT), the Privacy and Personal Information Protection Act 1998 (NSW), the Information Privacy Act 2009 (Qld), the Personal Information and Protection Act 2004 (Tas), and the Privacy and Data Protection Act 2014 (Vic).

1.3 Is there any sector-specific legislation that impacts data protection?

Privacy issues specific to the telecommunications sector are contained within the Telecommunications Act 1997 (Cth) (‘Telecommunications Act’) and the Telecommunications (Interception and Access) Act 1979 (Cth).

Information related to healthcare is further protected under the My Health Records Act 2012 (Cth) and Healthcare Identifiers Act 2010 (Cth). A multiplicity of state legislation also exists in relation to the protection of health-based privacy.

Businesses in industries such as financial services and gambling must comply with the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth) and Anti-Money Laundering and Counter-Terrorism Financing Rules.

1.4 What authority(ies) are responsible for data protection?

The Australian Communications and Media Authority (‘ACMA’) is the regulatory authority charged with enforcing the DNCRA and Spam Act, as well as having other functions under the Telecommunications Act.

The Commonwealth Attorney-General’s Department has responsibilities under the Telecommunications (Interception and Access) Act.

In coordination with the OAIC, the National Health and Medical Research Council has issued a number of binding guidelines in respect of privacy concerning health-related information.

The Australian Transaction Reports and Analysis Centre (‘AUSTRAC’) is the agency responsible for administering the Anti-Money Laundering and Counter-Terrorism Financing Act.

Various state and territory authorities also regulate privacy law issues in those jurisdictions. These include: the ACT Information Privacy Commissioner; the New South Wales Information and Privacy Commission; the Office of the Information Commissioner for the Northern Territory; the Queensland Office of the Information Commissioner; the South Australian Privacy Committee; the Tasmanian Ombudsman; the Office of the Victorian Information Commissioner; and the Office of the Information Commissioner for Western Australia.

2 Definitions

2.1 Please provide the key definitions used in the relevant legislation:

- **“Personal Data”**
  The analogous term used in the Privacy Act is ‘personal information’. This is defined in section 6 of the Privacy Act to mean information or an opinion about an identified individual, or an individual who is reasonably identifiable:
  a) whether the information or opinion is true or not; and
  b) whether the information or opinion is recorded in a material form or not.

- **“Processing”**
  The Privacy Act does not refer to ‘processing’, but regulates ‘dealing with’ personal information in terms of ‘use’ and ‘disclosure’ (see Part 3 of the APPs). Though both terms are not defined in the Privacy Act, the OAIC indicates that:
  - ‘Use’ means the handling or undertaking of activity in respect of information within its effective control.
  - ‘Disclose’ means to make information accessible to others outside the entity and to release subsequent handling of such information from the entity’s control.
“Controller”
The Privacy Act does not refer to ‘controllers’ but rather covers the information-processing activities of APP entities. APP entities include agencies and organisations. Agencies include:
- government ministers or departments;
- bodies established for a public purpose;
- bodies established by the Governor-General or a Minister;
- a person holding an office by appointment under an Act or by the Governor-General;
- a federal court; or
- the Australian Federal Police.
Organisations include:
- individuals;
- bodies corporate;
- partnerships;
- other unincorporated associations; and
- trusts.
Organisations do not include small business operators, registered political parties, agencies, or State and Territory authorities.

“Processor”
Whilst the term ‘processor’ is not used in the Privacy Act, the APPs naturally apply to APP entities to the extent that they hold personal information. According to the OAIC, this is sufficiently broad to encompass outsourced serviced providers which, for example, in Europe might be considered ‘processors’.

“Data Subject”
The Privacy Act regulates the processing of personal information about individuals, defined in section 6 to mean natural persons.

“Sensitive Personal Data”
‘Sensitive information’ is defined by section 6 of the Privacy Act to mean:

a) Personal information about an individual’s:
   i. racial or ethnic origin;
   ii. political opinions;
   iii. membership of a political association;
   iv. religious beliefs or affiliations;
   v. philosophical beliefs;
   vi. membership of a professional trade association;
   vii. membership of a trade union;
   viii. sexual orientation or practices; or
   ix. criminal record;

b) health information;

c) genetic information;
d) biometric information; or
e) biometric templates.

“Data Breach”
‘Eligible data breach’ is defined by section 26WE(2) of the Privacy Act as occurring where:
- there is unauthorised access to, or disclosure of, information (or it is lost in circumstances where such access or disclosure is likely to occur); and
- a reasonable person would conclude such access or disclosure would be likely to result in serious harm to any individual to which the information relates.

Other key definitions – please specify (e.g., “Pseudonymous Data”, “Direct Personal Data”, “Indirect Personal Data”).

“Collects”
As defined in section 6 of the Privacy Act, an entity collects personal information only if this is done for inclusion in a record or generally available publication.

“De-identified”
Personal information is de-identified if it is no longer about an identified individual or an individual who is reasonably identifiable.

“Employee record”
This means a record of personal information relating to the employment of an employee, including their health, resignation/termination, contact details, salary/wages, union/professional association membership, and taxation affairs.

“Holds”
An entity holds personal information if it possesses or controls a record that contains such information.

“Identification information”
Identification information about an individual means the person’s:
- full name;
- alias or previous name;
- date of birth;
- sex;
- current or last known address and two previous addresses;
- current or last known employer; or
- driver’s licence number.

“Record”
A record includes a document or electronic or other device. It does not, however, include:
- generally available public information;
- anything kept in a library, art gallery or museum for the purposes of reference, study or exhibition;
- Commonwealth records in the open access period;
- records in the care of the National Archives of Australia;
- documents placed in the memorial collection of the Australian War Memorial; or
- letters or articles transmitted by post.

3 Territorial Scope

3.1 Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to those laws?

Section 5B(1A) of the Privacy Act extends its application to acts done outside Australia by an organisation, or small business operator, with an Australian link. For businesses established outside Australia, an Australian link could cover situations where business is carried on in Australia and the personal information was collected or held in Australia. However, section 6A of the Privacy Act dictates that the APPs will not be breached by any conduct external to Australia that is required by an applicable foreign law.
4 Key Principles

4.1 What are the key principles that apply to the processing of personal data?

- **Transparency**
  APP 1 aims to ensure that personal information is managed in an open and transparent way. Entities are required to implement practices, procedures and systems to comply with the APPs and enable them to deal with enquiries/complaints in this regard. It also necessitates a clearly expressed privacy policy that is freely available.

- **Lawful basis for processing**
  Broadly speaking, the lawful basis upon which an entity may process personal data is the consent of the individual. However, the majority of the APPs contain limitations or extensions relating to the application of Commonwealth laws, records, and/or agreements. APP 3.5 specifies that personal information may only be collected by lawful and fair means.

- **Purpose limitation**
  Pursuant to APP 6, where an entity has collected personal information for a particular person, that information cannot then be used or disclosed for any further purpose other than with consent of the individual. This is limited, however, by certain defined exceptions, such as where the individual would hold a reasonable expectation of disclosure, where disclosure is required authorised by a court or tribunal, or where a certain permitted health situation exists (See APPs 6.2 and 6.3).

- **Data minimisation**
  The APPs address data minimisation in a piecemeal approach, combining a prohibition on reallocation of the purpose for holding information without consent (APP 6), limiting the collection of information to that which is reasonably necessary for the function in question (APP 3), and mandating destruction/de-identification where no purpose for use or disclosure of the information remains (APP 11).

- **Proportionality**
  Pursuant to APP 3, an APP entity may only collect personal information to the extent that it is reasonably necessary for, or directly related to, one or more of the entity’s functions or activities. For sensitive information, collection further requires the individual’s consent.

- **Retention**
  When an entity holds personal information, and no purpose for its use or disclosure remains, APP 11.2 requires the entity to destroy or de-identify the information. This does not apply to information on a Commonwealth record or required to be retained by law.

Further key principles – please specify

- **Collection of unsolicited personal information**
  Where an APP entity receives non-solicited personal information, APP 4 requires it to determine whether or not such information could have been solicited under APP 3. If this could not have been done (subject to certain limitations), the entity must destroy the information or ensure its de-identification.

- **Cross-border disclosure**
  Unless authorised, entities that intend to disclose personal information in a cross-border context must, pursuant to APP 8, take reasonable steps to ensure that the foreign entity receiving such information complies with the APPs. This is subject to exceptions, such as where that foreign entity is subject to a similar privacy regime under foreign law, or the information is being disclosed pursuant to a treaty obligation.

- **Government-related identifiers**
  APP 9 prohibits (with certain exceptions) the adoption, use or disclosure of government-related identifiers for individuals, by non-government organisations.

- **Quality of personal information**
  APP 10 mandates that personal information held, used, and disclosed should be accurate, up-to-date, and complete.

- **Security**
  Where an APP entity holds personal information, APP 11 dictates that it must take reasonable steps to protect this from misuse, interference, loss and unauthorised access, modification or disclosure.

5 Individual Rights

5.1 What are the key rights that individuals have in relation to the processing of their personal data?

- **Right to access to data/copies of data**
  Upon request from the concerned individual, an entity holding personal information must give that individual access to such information. This does not apply where information is held by a government agency that has a lawful reason for non-disclosure, or in certain circumstances such as where access would pose a serious threat to health or safety or would unreasonably impact the privacy of others.

- **Right to rectification of errors**
  APP 10 mandates that personal information held, used, and disclosed should be accurate, up-to-date, and complete. Pursuant to APP 13, upon request by an individual, an entity must take reasonable steps to correct any of that person’s information that is inaccurate, out-of-date, incomplete, irrelevant, or misleading.

- **Right to deletion/right to be forgotten**
  APP 11.2 requires that reasonable steps be taken to delete or de-identify personal information once its purpose(s) for use no longer exists. This is subject to the information not being in a Commonwealth record and the APP entity not being required by law to retain the information. Despite some discussion about legislative reform in this area, however, there is no right to be forgotten under Australian law, similar to the right under European law.

- **Right to object to processing**
  In practical terms, an individual’s power to restrict processing of their personal information is limited to their initial withholding of consent to the collection of such information. APP 2 requires that persons be allowed not to identify themselves when dealing with an APP entity (unless required/permits by law, or if this would be impractical). Additionally, APP 5 requires that individuals be notified before (or as soon as practicable after) their personal information is collected, thereby giving them the opportunity to object to such collection by disengaging with the entity.

- **Right to restrict processing**
  Whilst the APPs impose certain restrictions on how personal information can be dealt with (such as those relating to the purpose for which information is held (APPs 3 and 6)), there is no right bestowed on individuals to restrict the manner with which their information is dealt. Any such control held by an individual is largely relinquished upon the initial giving of consent to its collection.

- **Right to data portability**
  A broad right to data portability does not presently exist under Australian law (although, pursuant to APP 12, individuals can...
request a copy of their personal information held by an APP entity). However, the Australian Government is actively moving to progressively legislate this right – to be known as ‘consumer data right’ (‘CDR’) – into Australian law. CDR will first apply to the banking sector, and will allow persons to request that their data be shared with an accredited recipient. The Australian Competition and Consumer Commission will be the lead regulator of CDR.

- **Right to withdraw consent**

According to the OAIC, individuals should be provided with an easy and accessible process to withdraw their consent to the use or disclosure of their personal information. The withdrawal of consent invalidates formerly given consent being relied upon in relation to future use or disclosure of that person’s information. However, individuals must be advised of the implications of their consent being withdrawn.

- **Right to object to marketing**

APPs 7.2 and 7.3 require APP entities using personal information to engage in direct marketing to provide a simple means by which individuals may easily request to not receive such communications, which is drawn to the individual’s attention. If such a request is made, the entity must cease direct marketing to the individual.

- **Right to complain to the relevant data protection authority(ies)**

The OAIC is empowered to receive individual complaints about the handling of personal information. It can also recognise external dispute-resolution schemes (‘EDRS’) that handle particular privacy-related complaints. For example, from 1 November 2018 the Australian Financial Complaints Authority was recognised as an EDRS for the financial services industry.

**Other key rights – please specify**

- **Right to anonymity**

Pursuant to APP 2, individuals must have the option of not identifying themselves or using a pseudonym when dealing with APP entities, unless that entity is required/authorised by law to deal with individuals who have identified themselves, or if dealing with non-identified individuals would be impracticable.

- **Right to notification**

APP 5 mandates that individuals are notified of the collection of their personal information before, or as soon as practicable after, it occurs.

### 6 Registration Formalities and Prior Approval

#### 6.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?

There is no legal obligation on businesses to register with or notify the OAIC or any other bodies in relation to their data-processing activities in general. Specific obligations arise when eligible data breaches occur, as detailed in question 15. However, the OAIC has issued guidance to assist APP entities to prepare responses to any such breaches.

#### 6.2 If such registration/notification is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?

This is not applicable in Australia – please see question 6.1.

#### 6.3 On what basis are registrations/notifications made (e.g., per legal entity, per processing purpose, per data category, per system or database)?

This is not applicable in Australia – please see question 6.1.

#### 6.4 Who must register with/notify the data protection authority (e.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation)?

This is not applicable in Australia – please see question 6.1.

#### 6.5 What information must be included in the registration/notification (e.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes)?

This is not applicable in Australia – please see question 6.1.

#### 6.6 What are the sanctions for failure to register/notify where required?

This is not applicable in Australia – please see question 6.1.

#### 6.7 What is the fee per registration/notification (if applicable)?

This is not applicable in Australia – please see question 6.1.

#### 6.8 How frequently must registrations/notifications be renewed (if applicable)?

This is not applicable in Australia – please see question 6.1.

#### 6.9 Is any prior approval required from the data protection regulator?

This is not applicable in Australia – please see question 6.1.

#### 6.10 Can the registration/notification be completed online?

This is not applicable in Australia – please see question 6.1.

#### 6.11 Is there a publicly available list of completed registrations/notifications?

This is not applicable in Australia – please see question 6.1.
6.12 How long does a typical registration/notification process take?

This is not applicable in Australia – please see question 6.1.

7 Appointment of a Data Protection Officer

7.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.

Such an appointment is optional. The OAIC recommends that entities consider designating privacy officers that regularly report to their governance bodies as part of their obligations to implement practices, procedures and systems to ensure compliance with the APPs.

7.2 What are the sanctions for failing to appoint a Data Protection Officer where required?

This is not applicable in Australia – please see question 7.1.

7.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect of his or her role as a Data Protection Officer?

This is not applicable in Australia – please see question 7.1.

7.4 Can a business appoint a single Data Protection Officer to cover multiple entities?

In relation to government agencies, the OAIC recommends that privacy contact officers be of sufficient seniority to be involved in many aspects of the agency’s operations, including its decision-making processes.

7.5 Please describe any specific qualifications for the Data Protection Officer required by law.

This is not applicable in Australia – please see question 7.1.

7.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?

The OAIC recommends that privacy officers regularly report to their entity’s governance body. In relation to best practice for government agencies, the OAIC recommends that privacy contact officers should be at least at the executive level and:

- participate in the development of initiatives with a privacy impact;
- advise on the application of the Privacy Act;
- handle or supervise the handling of privacy complaints;
- train staff in relation to relevant aspects of the Privacy Act; and
- be the primary contact for the OAIC.

7.7 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?

No, registration/notification is not required.

7.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?

No. The OAIC requires privacy policies to be high-level documents that are not expected to contain detail about all the entity’s practices, procedures and systems relating to management of personal data.

8 Appointment of Processors

8.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?

As the APPs do not specifically refer to ‘processors’, this is not strictly the case.

However, although the Privacy Act and APPs do not refer explicitly to processors, the OAIC’s view is that APP entities which are outsourced service providers holding personal information, even if not controlling it as such, must comply with this legal regime.

Where the processor is located overseas, the regulation of foreign information transfer, as detailed below in question 8, will apply.

8.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?

Although not applicable, entering such agreements remains best practice. In the context of cross-border disclosure, the OAIC recommends that such contracts cover:

- the type of personal information and purpose for its disclosure;
- a requirement that the recipient of the information complies with the APPs;
- the complaints-handling process; and
- a requirement as to the implementation of a data-breach response plan.

9 Marketing

9.1 Please describe any legislative restrictions on the sending of electronic direct marketing (e.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?).

APP 7.1 imposes a general prohibition on the use of personal information for the purpose of direct marketing. This does not apply where the organisation provides a simple means through which the individual can opt-out of the marketing and:

- the information was collected in circumstances that would give rise to reasonable expectation of the information being used in such marketing; or
- the individual has consented to the receipt of such marketing.
9.2 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.).

The DNCRA prohibits most unsolicited telemarketing calls and fax messages to numbers placed on a national Do Not Call Register, without the consent of the person/organisation being contacted. The Spam Act prescribes the sending of most unsolicited and non-consensual electronic messages. Some exceptions to this prohibition are electronic messages by government bodies, political parties and charities.

9.3 Do the restrictions noted above apply to marketing sent from other jurisdictions?

The Spam Act regulates the sending of commercial electronic messages with ‘an Australian link’. This covers messages that:

- originate in Australia;
- were sent, or authorised by, an individual/organisation physically present in Australia, or with central management and control in Australia, when the message was sent;
- were accessed by a computer, server or device that is located in Australia;
- is connected to an electronic account-holder that is either an individual present in Australia or an organisation carrying on business or activities in Australia when the message is accessed; or
- if unable to be delivered due to the non-existence of a delivery address would, had the address existed, reasonably likely have been accessed using a computer, server, or device located in Australia.

The DNCRA concerns telephone calls and fax messages sent to ‘an Australian number’. This means numbers that are specified in the plan set out in the Telecommunications Act and for use in connection with the supply of carriage services to the public in Australia. Section 9 of the DNCRA also expressly extends the legislation’s application to acts done outside Australia’s territory.

9.4 Is/are the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?

Yes. The ACMA, which is the regulatory authority charged with enforcing the DNCRA and Spam Act, regularly publishes its actions taken in discharging these functions.

For example, in February 2019 an e-marketing company was fined almost $40,000 for breaches of the Spam Act arising from third party marketing. Further, in January 2019 the ACMA penalised a telecommunications provider over $50,000 for making telemarketing calls to numbers on the Do Not Call Register.

9.5 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?

Yes. However, when doing so, the purchaser must ensure their compliance with APP 7.3. This requires that persons have either consented to receipt of marketing or that it is impractical to obtain such consent and that in each communication recipients are provided, via a prominent statement, with a simple means to ‘opt out’ of these communications.

Under APP 7.6(c), individuals may request to be advised of the source of their personal information used or disclosed in relation to direct marketing.

9.6 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?

Breaches of the DNCRA may result in corporate liability for civil penalties up to $2.1 million, and individual liability for up to $420,000 per day. This will depend on the number of breaches and history of the actor. Compensation can also be ordered where a victim has suffered loss or damage.

This penalty regime (and maximum sanctions) is largely mirrored in respect of the Spam Act. Additionally, the Privacy Act contains numerous provisions addressing the payment of civil penalties, fines and compensation to victims.

10 Cookies

10.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).

There is no specific legal regime that applies to cookies. Whilst the information collected through the use of cookies is often generalised, where it rises to the level of enabling identification of an individual, the use of cookies will be subject to the APPs.

10.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?

Whilst the APPs do not (in theory) apply differently to different cookies, the OAIC has issued public guidance about their distinctive operations and how individuals can adjust their browsing preferences accordingly.

10.3 To date, has/have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?

To date, the OAIC has not done so.

10.4 What are the maximum penalties for breaches of applicable cookie restrictions?

Not applicable.

11 Restrictions on International Data Transfers

11.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.

The transfer of personal information to jurisdictions outside Australia is governed by APP 8. APP 8.1 requires that entities must take reasonable steps to ensure that a foreign recipient of personal information complies with the APPs. According to APP 8.2, however, this is not necessary where:
11.2 **Please describe the mechanisms businesses typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).**

The OAIC espouses an expectation that, to take the necessary reasonable steps, entities transferring personal information to foreign recipients will enter into enforceable contracts requiring compliance with the APPs.

Under section 16C of the Privacy Act, if an entity has disclosed personal information on the basis of a belief that the foreign recipient will be APP-compliant (i.e. under APP 8.1), the Australian entity bears legal responsibility for any breaches of the APPs by the recipient.

11.3 **Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.**

No. The entity itself must assess whether or not the foreign recipient will comply with the APPs or is subject to a similar privacy regime and, if necessary, seek the individual’s consent only.

12 **Whistle-blower Hotlines**

12.1 **What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?**

Protections of corporate whistle-blowers are provided for in the Corporations Act. This relates to the reporting of breaches of the Corporations Act or the *Australian Securities and Investments Commission Act 2001* (Cth). Whistle-blowers are protected from any litigation (civil or criminal), employment termination or victimisation as a result of their actions.

To qualify for these protections, a person must:

- be an officer, employee, or contractor of the company in question;
- make disclosure to a company auditor (or member of the audit team), officer or senior manager, person authorised to receive whistle-blower disclosure, or the Australian Securities and Investments Commission;
- give their name when making disclosure;
- have reasonable grounds to suspect a breach of relevant law may have occurred; and
- make the disclosure in good faith.

12.2 **Is anonymous reporting prohibited, strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do businesses typically address this issue?**

To qualify as a whistle-blower under the Corporations Act, a person must provide their name when making disclosure.

On the other hand, whilst the Privacy Act is silent as to anonymous reporting, the OAIC requires the contact details of persons complaining to it about privacy breaches.

13 **CCTV**

13.1 **Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?**

In relation to federal government agencies, the *Surveillance Devices Act 2004* (Cth) provides broad authority for the use of ‘optical surveillance devices’ by law enforcement without a warrant. Whilst the use of CCTV specifically is regulated by the States, New South Wales, for example, mandates that CCTV be ‘obvious and suitably visible’, preferably with signage advising of its presence. On the other hand, Queensland requires that entities take ‘reasonable steps’ to make persons aware of their purpose and authority for using camera surveillance.

13.2 **Are there limits on the purposes for which CCTV data may be used?**

Again, this varies from state to state. However, as examples, both New South Wales and Queensland limit the collection of personal information by entities through CCTV to circumstances directly related to one of their functions.

14 **Employee Monitoring**

14.1 **What types of employee monitoring are permitted (if any), and in what circumstances?**

This varies by state. For example, New South Wales has dedicated legislation mandating consent or notice to legitimise the conduct of employee surveillance. On the other hand, Victorian law prohibits workplace surveillance in certain locations (e.g. bathrooms) but otherwise provides no additional restrictions over the general legal framework. The Queensland Law Reform Commission is currently examining workplace surveillance, with a review expected to be completed in 2020.

As best practice, the Australian Fair Work Ombudsman recommends that employers adhere to privacy standards consistent with the APPs. It is also advised that employers clearly advise employees of policies in relation to internet, phone and email use, as well as monitoring.
14.2 Is consent or notice required? Describe how employers typically obtain consent or provide notice.

In New South Wales, employees must be given at least 14 days’ notice, or notice prior to their commencing work. This must include various details about the nature and extent of the monitoring.

14.3 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?

There is no requirement under Australian privacy law for employee representatives or trade unions to be notified or consulted regarding employee monitoring.

15 Data Security and Data Breach

15.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?

APP 11 stipulates that entities must take reasonable steps to protect personal information:
- from misuse, interference, and loss; and
- from unauthorised access, modification or disclosure.

The OAIC has stated that any APP entity that holds personal information (even those that could be considered processors) is responsible for compliance with the APPs. In cases of cross-border disclosure, see the discussion in section 11 above.

15.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

Yes. The Privacy Act requires entities to notify the OAIC whenever an ‘eligible data breach’ occurs. Eligible data breaches involve unauthorised access to, or disclosure of, personal information that is likely to result in serious harm which the entity has not been able to negate with remedial action.

If it is not clear whether such a breach has occurred, entities must investigate in order to form their own assessment. The entity must take all reasonable steps to complete this within 30 days of becoming aware of information giving rise to its suspicion of the breach.

15.3 Is there a legal requirement to report data breaches to affected data subjects? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

Yes. The notification requirements referred to above in relation to the OAIC also apply to individuals whose personal data has been the subject of any such breach.

15.4 What are the maximum penalties for data security breaches?

The penalties for breaches of the Privacy Act, imposable by the OAIC, include requiring apologies and proposals of remedial measure, as well as civil penalties ranging in value up to $2.1 million.

16 Enforcement and Sanctions

16.1 Describe the enforcement powers of the data protection authority(ies).

Where the OAIC receives a privacy complaint, its powers under the Privacy Act include:
- making preliminary enquiries of any person;
- assessing an entity’s privacy practices and providing it with non-binding recommendations;
- accepting an enforceable undertaking;
- providing directions to an entity following the making of a determination in respect of the investigated action;
- bringing proceedings to enforce an undertaking or determination;
- seeking a court injunction to prevent a breach of the Privacy Act occurring;
- applying to a court for the imposition of a civil penalty order; and
- reporting to the Minister about the investigation (in certain circumstances, this is mandatory).

Criminal sanctions, such as a fine or term of imprisonment up to 12 months, may result from a failure to appear before, give information to, or provide false or misleading information to the OAIC when required to do so under the Act.

16.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?

The OAIC has the power to make legally binding rules and approve legally binding guidelines in respect of privacy issues. Current such instruments concern issues such as use of Tax File Numbers, medical research and genetic information. These instruments do not require any type of authorisation by court order.

The above instruments cover discrete issues only and otherwise the OAIC’s ‘hard’ powers relate to specific cases, through making determinations in respect of particular complaints and accepting enforceable undertakings.
16.3 Describe the data protection authority’s approach to exercising those powers, with examples of recent cases.

In respect of the abovementioned guidelines, the OAIC has approved those issued by the National Health and Medical Research Council. The rules, on the other hand, are issued by the OAIC. Where a complaint is made in respect of an alleged privacy breach, if conciliation does not resolve the matter, the OAIC may determine whether a breach has occurred and, if so, what remedies should be ordered. In 2018, the OAIC found that a superannuation fund had unlawfully disclosed personal information of its members to third parties. As a result, an apology was ordered.

In other cases where an entity has cooperated with an investigation/enquiry by the OAIC, or in response to a privacy complaint, the OAIC may accept an enforceable undertaking to ensure future compliance with privacy law. In late 2018, the OAIC accepted an undertaking from the Department of Health following the release of data concerning patients’ claims for public medical benefits.

16.4 Does the data protection authority ever exercise its powers against businesses established in other jurisdictions? If so, how is this enforced?

Whilst the predominant focus of the OAIC is directed towards businesses and companies established domestically, the OAIC does take action in respect of foreign organisations. For example, in 2016 the OAIC, having worked with the Privacy Commissioner of Canada, obtained an enforceable undertaking from a Canadian-based media company in respect of concerns over security of personal information, retention and accuracy of data, as well as compliance reporting, monitoring and enforcement.

17 E-discovery / Disclosure to Foreign Law Enforcement Agencies

17.1 How do businesses typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?

Although APP 8.2 allows the disclosure of information to an overseas recipient where required/authorised by law, this is restricted to Australian legislation and courts/tribunals. It does not apply to requests from foreign law enforcement agencies, which remain subject to APP 8.1 (requiring the taking of reasonable steps to ensure that the overseas recipient does not breach the APPs).

Under section 6A(4) of the Privacy Act, a business acting outside Australia, and as required by an applicable foreign law, will not breach the APPs. This is notwithstanding the extraterritorial reach of the Privacy Act, detailed above.

Australia is also party to a number of international treaties and conventions that relate to the sharing of data across national borders. Although concerning the actions of public bodies, not businesses, they are of central relevance to the sharing of Australian information with foreign law enforcement. These instruments include the following examples:

A. The ‘Five Eyes’ is an intelligence pact between Australia, the United States, the United Kingdom, New Zealand and Canada, all parties to the UKUSA Agreement. Part of this arrangement is ‘critical information sharing’ between the nations that relates to issues of law enforcement, border protection and criminal justice. These partners also share information concerning financial sector intelligence.

B. Australia is party to over 25 bilateral mutual legal assistance treaties with foreign nations. All these treaties contain provisions explicitly contemplating the exchange of information between governments in relation to criminal matters.

C. Australia is a party to the multilateral 2001 Budapest Convention on Cybercrime. Over 70 nations are party to this treaty. The Budapest Convention covers a range of issues related to international cyber-crime, including requests to/from foreign states for the seizure, collection and interception of computer data. Article 26 specifically contemplates the spontaneous sharing of information between nations, without any prior request, that may be used in the investigation or prosecution of cyber-crime offences.

D. Australia is also party to a number of Taxation Information Exchange Agreements (‘TIEAs’) with states outside the Organisation for Economic Cooperation and Development. TIEAs facilitate the exchange of information between countries concerning taxation matters and are aimed at combatting international tax avoidance.

17.2 What guidance has/have the data protection authority(ies) issued?

The OAIC has issued guidance to businesses on this issue as part of its commentary to APP 8. The OAIC recommends that APP entities notify the individual that it may be required to disclose personal information under a foreign law, and that this would not breach the APPs. It is also suggested that any entity involved in regular foreign disclosure of personal information should include this in its notice under APP 5.

In relation to information shared through international treaties and conventions, such as those described above, Australia is party to numerous international agreements governing the protection of information shared across borders. These agreements cover issues such as security classification, protective measures, and procedures for the exchange of such information.

18 Trends and Developments

18.1 What enforcement trends have emerged during the previous 12 months? Describe any relevant case law.

A major recent development in Australian privacy law was the passing of the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 (Cth) (‘Assistance and Access Act’) on the final sitting day of Federal Parliament for 2018, following a period of public consultation. The Assistance and Access Act contains an array of legislative reforms granting government agencies greater powers to access computer data and communications.

A prominent aspect of the Act is the power of government agencies to issue compulsory Technical Assistance Notices (‘TAN’) and Technical Capability Notices (‘TCN’) to communications providers, essentially requiring private organisations to aid public law enforcement actions. The issuing of a TAN will require a provider to assist an agency through action such as removing electronic protections (e.g. decrypting communications), providing technical information, utilising software nominated by the agency, or facilitating access to devices/service, etc. On the other hand, a TCN requires a communications provider to develop a new capability to...
assist the government agency, and can cover anything that could be the subject of a TAN, except the removal of electronic protections. The scope of legislation affected by the Assistance and Access Act is broad, stretching from the Crimes Act 1914 to the Mutual Assistance in Criminal Matters Act 1987, to the Telecommunication Act 1997. Although passed into law, the Parliamentary Joint Committee on Intelligence and Security is due to further report on this Act in April 2019.

18.2 What “hot topics” are currently a focus for the data protection regulator?

Health records, in particular the introduction of the ‘My Health Record’ system – containing online summaries of personal health information – have been the subject of much recent attention, including the extension into 2019 of a public opt-out period. The OAIC has issued a wide array of public guidance on privacy issues that may be associated with this system. The early operation of the Notifiable Data Breaches scheme continues to receive attention from the OAIC, including through the publication of a guide for entities dealing with such data breaches.

Acknowledgment

The authors would like to thank Liam MacAndrews, Solicitor, for his invaluable contribution to the writing of this chapter. Liam assists the Partners on international criminal law cases and cross-border investigations.

Dennis Miralis
Nyman Gibson Miralis
Level 9, 299 Elizabeth Street
Sydney NSW 2000
Australia
Tel: +61 2 9264 8884
Email: dm@ngm.com.au
URL: www.ngm.com.au

Dennis Miralis is a leading Australian defence lawyer who specialises in international criminal law, with a focus on complex multi-jurisdictional regulatory investigations and prosecutions. His areas of expertise include bribery and corruption, global tax investigations, proceeds of crime, anti-money laundering, worldwide freezing orders, cybercrime, national security law, Interpol Red Notices, extradition and mutual legal assistance law. Dennis advises individuals and companies under investigation for economic crimes both locally and internationally. He has extensive experience in dealing with all major Australian and international investigative agencies.

Phillip Gibson
Nyman Gibson Miralis
Level 9, 299 Elizabeth Street
Sydney NSW 2000
Australia
Tel: +61 2 9264 8884
Email: pg@ngm.com.au
URL: www.ngm.com.au

Phillip Gibson is one of Australia’s leading criminal defence lawyers, with over 30 years of experience in all areas of criminal law. Phillip has significant experience in transnational cases across multiple jurisdictions often involving: white-collar and corporate crime; assets forfeiture; money laundering and proceeds of crime; extradition; mutual assistance; Royal Commissions; bribery and corruption; and ICAC and Crime Commissions matters. He has extensive experience in dealing with all major Australian and international investigative agencies.

Nyman Gibson Miralis is an international award-winning criminal defence law firm based in Sydney, Australia. For over 50 years it has been leading the market in all aspects of general, complex and international crime, and is widely recognised for its involvement in some of Australia’s most significant criminal cases.

Our international law practice focuses on white-collar and corporate crime, transnational financial crime, bribery and corruption, international money laundering, cybercrime, international asset freezing or forfeiture, extradition and mutual assistance law.

Nyman Gibson Miralis strategically advises and appears in matters where transnational cross-border investigations and prosecutions are being conducted in parallel jurisdictions, involving some of the largest law enforcement agencies and financial regulators worldwide.

Working with international partners, we have advised and acted in investigations involving the USA, Canada, the UK, the EU, China, Hong Kong, Singapore, Taiwan, Macao, Vietnam, Cambodia, Russia, Mexico, South Korea, British Virgin Islands, New Zealand and South Africa.
Chapter 7

Austria

Herbst Kinsky Rechtsanwälte GmbH

Dr. Sonja Hebenstreit

1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

As of 25 May 2018, the principal data protection legislation in the EU is Regulation (EU) 2016/679 (General Data Protection Regulation – “GDPR”). The GDPR repealed Directive 95/46/EC (“Data Protection Directive”) and leads to an increased (though not total) harmonisation of data protection law across the EU Member States.

The Data Protection Act Adaptation Act 2018 (Datenschutzgesetz-Anpassungsgesetz 2018), published in the Federal Law Gazette (Bundesgesetzblatt – “BGBl.”) I Nr. 120/2017, amended the former Data Protection Act 2000 (Datenschutzgesetz 2000) in accordance with the GDPR and entered into force on 25 May 2018 as the Austrian Data Protection Act (Datenschutzgesetz – “DSG”, as last amended by BGBl. I Nr. 14/2019). Furthermore, Directive (EU) 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, was implemented into Austrian law by the Data Protection Act Adaptation Act 2018.

1.2 Is there any other general legislation that impacts data protection?

Labour law has a significant impact on data protection. As the DSG does not contain a systematic regulation of data protection in the context of employment, the principal legislation on data protection in this context is the Austrian Labour Constitution Act (Arbeitsverfassungsgesetz – “ArbVG”); in particular, sections 96 and 96a ArbVG. For certain data processing activities (e.g., the implementation of control systems such as whistle-blowing mechanisms), the consent of the works council is mandatory (please see section 14 below). The relevant provisions of the ArbVG apply in addition to the “general” data protection laws (GDPR and DSG) with regard to employee data protection.

1.3 Is there any sector-specific legislation that impacts data protection?

Other sector-specific legislation can, inter alia, be found in the Telecommunications Act 2003, which contains the implementation of the EU Data Protection Directive on Electronic Communications (e.g., provisions regarding commercial electronic communication, cookies, etc.), as well as in the Austrian Banking Act (banking secrecy). Many other laws have been adapted due to the GDPR’s entry into force, namely by two Material Data Protection Adaptation Acts (1. Materien-Datenschutz-Anpassungsgesetz 2018, BGBl. I Nr. 32/2018; and 2. Materien-Datenschutz-Anpassungsgesetz 2018, BGBl. I Nr. 37/2018).

1.4 What authority(ies) are responsible for data protection?

The Datenschutzbehörde (“DSB”) is the national independent supervisory authority in Austria (see section 18 para 1 DSG). Another institution is the Data Protection Council (Datenschutzrat), which is responsible for advising the Federal Government and the State Governments on requests concerning data protection law (section 14 et seq. DSG). Until 24 May 2018, Austrian data protection law required the registration of data applications with the DSB. This data processing register (Datenverarbeitungsregister) will be continued for archiving purposes until 31 December 2019.

2 Definitions

2.1 Please provide the key definitions used in the relevant legislation:

- “Personal Data” means any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
- “Processing” means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
- “Controller” means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
Do the data protection laws apply to businesses established outside the EU?

The GDPR applies to businesses that are established in any EU Member State, and that process personal data (either as a controller or processor, and regardless of whether or not the processing takes place in the EU) in the context of that establishment.

A business that is not established in any Member State, but is subject to the laws of a Member State by virtue of public international law, is also subject to the GDPR.

The GDPR applies to businesses outside the EU if they (either as controller or processor) process the personal data of EU residents in relation to: (i) the offering of goods or services (whether or not in return for payment) to EU residents; or (ii) the monitoring of the behaviour of EU residents (to the extent that such behaviour takes place in the EU).

Further, the GDPR applies to businesses established outside the EU if they monitor the behaviour of EU residents (to the extent such behaviour takes place in the EU).

### 4 Key Principles

#### 4.1 What are the key principles that apply to the processing of personal data?

- **Transparency**
  Personal data must be processed lawfully, fairly and in a transparent manner. Controllers must provide certain minimum information to data subjects regarding the collection and further processing of their personal data. Such information must be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

- **Lawful basis for processing**
  Processing of personal data is lawful only if, and to the extent that, it is permitted under EU data protection law. The GDPR provides an exhaustive list of legal bases on which personal data may be processed, of which the following are the most relevant for businesses: (i) consent of the data subject for one or more specific purposes (for the requirements of an effective consent see definition above); (ii) contractual necessity (i.e., the processing is necessary for the performance of a contract to which the data subject is a party, or for the purposes of pre-contractual measures taken at the data subject’s request); (iii) compliance with legal obligations (i.e., the controller has a legal obligation, under the laws of the EU or an EU Member State, to perform the relevant processing); or (iv) legitimate interests (i.e., the processing is necessary for the purposes of legitimate interests pursued by the controller, except where the controller’s interest are overridden by the interests, fundamental rights or freedoms of the affected data subjects). Please note that businesses require stronger grounds to process sensitive personal data. The processing of sensitive personal data is only permitted under certain conditions, of which the most relevant for businesses are: (i) explicit consent of the affected data subject; (ii) the processing is necessary in the context of employment or social security law; or (iii) the processing is necessary for the establishment, exercise or defence of legal claims.

- **Purpose limitation**
  Personal data may only be collected for specified, explicit and legitimate purposes and must not be further processed in a manner that is incompatible with those purposes. If a controller wishes to use the relevant personal data in a manner that is incompatible with those purposes for which they were initially collected, it must: (i) inform the data subject of such new processing; and (ii) be able to rely on a lawful basis as set out above.

- **Data minimisation**
  The procession of personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which those data are processed. A business should only process the personal data that it actually needs to process in order to achieve its processing purposes.

- **Proportionality**
  The requirement of proportionality (of data processing) is reflected in the GDPR in many provisions, e.g., in Art 5 para 1 lit e or Art 9 para 2 lit g GDPR. Furthermore, the principle of proportionality is explicitly mentioned in Article 84 GDPR with regard to penalties for violations of the GDPR, which need to be “effective, proportionate and dissuasive”.

- **Retention**
  Personal data must be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. If those purposes have ceased, personal data should be irreversibly deleted or anonymised.

- **Other key principles – please specify**

- **Accuracy**
  Personal data must be accurate and, where necessary, kept up to date. A business must take every reasonable step to ensure that personal data that are inaccurate are either erased or rectified without delay.

- **Data security**
  Personal data must be processed in a manner that ensures appropriate security of those data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

- **Accountability**
  The controller is responsible for, and must be able to demonstrate, compliance with the data protection principles set out above. In particular, the controller is obliged to implement such new processing; and (ii) be able to rely on a lawful basis as set out above.
appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with the GDPR.

5 Individual Rights

5.1 What are the key rights that individuals have in relation to the processing of their personal data?

- **Right to access to data/copies of data**
  A data subject has the right to obtain from a controller the following information in respect of the data subject’s personal data: (i) confirmation of whether, and where, the controller is processing the data subject’s personal data; (ii) information about the purposes of the processing; (iii) information about the categories of data being processed; (iv) information about the categories of recipients with whom the data may be shared; (v) information about the period for which the data will be stored (or the criteria used to determine that period); (vi) information about the existence of the rights of the rights to erasure, to rectification, to restriction of processing and to object to processing; (vii) information about the existence of the right to complain to the relevant data protection authority; (viii) information about the data where the data were not collected from the data subject, information as to the source of the data; and (ix) information about the existence of, and an explanation of the logic involved in, any automated processing that has a significant effect on the data subject.
  Additionally, the data subject may request a copy of the personal data being processed.

- **Right to rectification of errors**
  Controllers must ensure that inaccurate or incomplete data are erased or rectified. Data subjects have the right to rectification of inaccurate personal data.

- **Right to deletion/right to be forgotten**
  Data subjects have the right to erasure of their personal data (the “right to be forgotten”) if: (i) the data are no longer needed for their original purpose and no new lawful purpose exists; (ii) the lawful basis for the processing is the data subject’s consent, the data subject withdraws that consent, and no other lawful ground exists; (iii) the data subject exercises the right to object, and the controller has no overriding grounds for continuing the processing; (iv) the data have been processed unlawfully; or (v) erasure is necessary for compliance with EU law or national data protection law.

- **Right to object to processing**
  Data subjects have the right to object, on grounds relating to their particular situation, to the processing of personal data where the basis for that processing is either public interest or legitimate interest of the controller. The controller must cease such processing unless it demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the relevant data subject or requires the data in order to establish, exercise or defend legal rights.

- **Right to restrict processing**
  Data subjects have the right to restrict the processing of personal data, which means that the data may only be held by the controller, and may only be used for limited purposes if: (i) the accuracy of the data is contested (and only for as long as it takes to verify that accuracy); (ii) the processing is unlawful and the data subject requests restriction (as opposed to exercising the right to erasure); (iii) the controller no longer needs the data for their original purpose, but the data are still required by the controller to establish, exercise or defend legal rights; or (iv) verification of overriding grounds is pending, in the context of an erasure request.

- **Right to data portability**
  Data subjects have a right to receive a copy of their personal data in a commonly used machine-readable format, and transfer their personal data from one controller to another or have the data transmitted directly between controllers.

- **Right to withdraw consent**
  A data subject has the right to withdraw their consent at any time. The withdrawal of consent does not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject must be informed of the right to withdraw consent. It must be as easy to withdraw consent as to give it.

- **Right to object to marketing**
  Data subjects have the right to object to the processing of personal data for the purpose of direct marketing, including profiling.

- **Right to complain to the relevant data protection authority(ies)**
  Data subjects have the right to lodge complaints concerning the processing of their personal data with the data protection authority in Austria, if the data subjects live in Austria or the alleged infringement occurred in Austria.

**Other key rights – please specify**

- **Right to basic information**
  Data subjects have the right to be provided with information on the identity of the controller, the reasons for processing their personal data and other relevant information necessary to ensure the fair and transparent processing of personal data.

- **Right not to be subject to automated individual decision-making**
  Data subjects have the right not to be subject to a decision based solely on automated processing of data (including profiling), which produces legal effects or similarly significantly affects for the data subject. This right applies unless a decision: (i) is necessary for entering into, or performance of, a contract between the data subject and the controller; (ii) is authorised by Union or Member State law to which the controller is subject and which lays down suitable measures to safeguard the data subject’s rights and legitimate interests; or (iii) is based on explicit consent. However, in these cases further requirements and exceptions apply.

6 Registration Formalities and Prior Approval

6.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?

Until 24 May 2018, every processing activity required prior notification to the DSB (and in some cases even prior approval), unless a legal exception applied. As from 25 May 2018, the DSG no longer contains any such general notification obligations. The data processing register will be continued for archiving purposes until 31 December 2019. The DSG provides, in its sections 7 and 8, specific requirements for prior approval of the DSB: (a) in the context of data processing in the public interest for the purposes of archiving, scientific or historical research or statistics (section 7 DSG); and (b) in the context of processing address data of data subjects for the purposes of an important public interest regarding the notification or interview of those subjects (section 8 DSG).
In line with the principle of accountability, any controller and processor now has to keep a record detailing all processing activities. This record serves the purpose of proving compliance with the GDPR and has to be presented to the DSB at the request of the authority. This obligation does not apply to organisations that employ less than 250 persons unless the processing activities are likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data or personal data relating to criminal convictions and offences.

The DSB has stated in its official guideline to the GDPR (the latest version issued in January 2019) that all documentation to be provided to the DSB in the course of an examination proceeding (e.g., processing register, data protection impact assessment (“DPIA”)) needs to be in German.

6.2 If such registration/notification is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?

Please see question 6.1 above.

6.3 On what basis are registrations/notifications made (e.g., per legal entity, per processing purpose, per data category, per system or database)?

Please see question 6.1 above.

6.4 Who must register with/notify the data protection authority (e.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation)?

Please see question 6.1 above.

6.5 What information must be included in the registration/notification (e.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes)?

Please see question 6.1 above.

6.6 What are the sanctions for failure to register/notify where required?

Please see question 6.1 above.

6.7 What is the fee per registration/notification (if applicable)?

Please see question 6.1 above.

6.8 How frequently must registrations/notifications be renewed (if applicable)?

Please see question 6.1 above.

6.9 Is any prior approval required from the data protection regulator?

Please see question 6.1 above.

6.10 Can the registration/notification be completed online?

Please see question 6.1 above.

6.11 Is there a publicly available list of completed registrations/notifications?

Please see question 6.1 above.

6.12 How long does a typical registration/notification process take?

Please see question 6.1 above.

7 Appointment of a Data Protection Officer

7.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.

The appointment of a Data Protection Officer for controllers or processors of the private sector is only mandatory if their core activities include: (i) large-scale regular and systematic monitoring of individuals; or (ii) large-scale processing of sensitive personal data.

If a business designates a Data Protection Officer voluntarily, the requirements of the GDPR apply as though the appointment were mandatory.

Austria has not made use of the possibility offered in Article 37 para 4 GDPR and has not provided for any further mandatory Data Protection Officer designation requirements.

7.2 What are the sanctions for failing to appoint a Data Protection Officer where required?

Under circumstances where an appointment of a Data Protection Officer is mandatory, failure to comply with such obligation may result in the wide range of penalties available under the GDPR. In particular, the controller or processor is subject to an administrative fine of the higher of up to EUR 10 million or 2% of the annual turnover of the respective controller, according to Article 83 para 4 GDPR.

7.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect of his or her role as a Data Protection Officer?

The appointed Data Protection Officer should not be dismissed or penalised for performing his tasks (although no general dismissal protection exists) and should report directly to the highest management level of the controller or processor.
In accordance with section 5 DSG, the Data Protection Officer is bound by secrecy. In particular, the identity of any person who has contacted the Data Protection Officer has to be kept confidential. In case the respective data subject has a privilege to refuse to give legal evidence and has made use of such privilege, the Data Protection Officer may not provide any information regarding the respective data.

### 7.4 Can a business appoint a single Data Protection Officer to cover multiple entities?

A group of undertakings may appoint a single data protection officer, provided that this person is easily accessible from each establishment.

### 7.5 Please describe any specific qualifications for the Data Protection Officer required by law.

The Data Protection Officer may be a staff member of the controller or processor or fulfil the tasks on the basis of a service contract, should be appointed on the basis of professional qualities, and should have an expert knowledge of data protection law and practices. The Data Protection Officer should have the ability to perform the tasks outlined in question 7.6 below. While this is not strictly defined, it is clear that the level of expertise required will depend on the circumstances. For example, the involvement of large volumes of sensitive personal data will require a higher level of knowledge.

### 7.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?

A Data Protection Officer should be involved in all issues which relate to the protection of personal data. The GDPR outlines the minimum tasks required by the Data Protection Officer, which include: (i) informing the controller, processor and their relevant employees who process data of their obligations under the GDPR; (ii) monitoring compliance with the GDPR, national data protection legislation and internal policies in relation to the processing of personal data, including internal audits; (iii) advising on DPIAs and the training of staff; and (iv) co-operating with the data protection authority and acting as the authority’s primary contact point for issues related to data processing.

### 7.7 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?

Yes. The controller or processor must notify the data protection authority of the contact details of the designated Data Protection Officer.

### 7.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?

The Data Protection Officer does not necessarily need to be named in the public-facing privacy notice. However, the contact details of the Data Protection Officer must be notified to the data subject when personal data relating to that data subject are collected. As a matter of good practice, the Article 29 Working Party (“WP29”) recommends that both the data protection authority and employees should be notified of the name and contact details of the Data Protection Officer.

### 8 Appointment of Processors

#### 8.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?

Yes. The business that appoints a processor to process personal data on its behalf is required to enter into a written agreement with the processor, which sets out the subject matter and the duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects, and the obligations and rights of the controller (i.e. the business).

It is essential that the processor appointed by the business complies with the GDPR. For transfer of personal data to processors outside the EU, please see question 11.2 below.

#### 8.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?

The processor must be appointed under a binding agreement in writing, which sets out the subject matter and duration as well as the nature and purpose of the processing, the type of personal data and categories of data subjects, and the obligations and rights of the controller. The contractual terms must stipulate that the processor: (i) only acts on the documented instructions of the controller; (ii) imposes confidentiality obligations on all employees; (iii) ensures the security of personal data that it processes; (iv) abides by the rules regarding the appointment of sub-processors; (v) implements measures to assist the controller with guaranteeing the rights of data subjects; (vi) assists the controller in obtaining approval from the Data Protection Officer; (vii) either returns or destroys the personal data at the end of the relationship (except as required by EU or Member State law); and (viii) provides the controller with all information necessary to demonstrate compliance with the GDPR.

### 9 Marketing

#### 9.1 Please describe any legislative restrictions on the sending of electronic direct marketing (e.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient)?

According to section 107 para 2 Austrian Telecommunications Act (Telekommunikationsgesetz 2003, containing the implementation of Directive 2002/58/EC, as amended; hereinafter “TKG”), the sending of electronic mail – including SMS messages – without the recipient’s prior consent shall not be permitted if the sending takes place for purposes of direct marketing. Such prior consent is not required if:

- contact details for the communication were obtained in the context of a sale or a service to the recipient;
- the communication is transmitted for the purpose of direct marketing of the sender’s own similar products or services;
- the recipient clearly and distinctively has, at the time the electronic contact information was collected and furthermore on the occasion of each contact, been given the opportunity to object, free of charge and in an easy manner, to such use of electronic contact details; and
9.2 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.).

According to section 107 para 1 TKG, marketing by telephone, including facsimile transmissions for marketing purposes, shall not be permitted without the prior consent of the subscriber. Please note that prior consent may not be received in the course of the first call, but must be obtained in advance. For marketing by post, no restrictions (as applicable for calls or emails) apply.

9.3 Do the restrictions noted above apply to marketing sent from other jurisdictions?

If unlawful direct marketing actions have not been committed in Austria, they shall be considered as having been committed in the place where the call reaches the subscriber’s line. As a result, this means that any direct marketing action is judged according to the aforementioned rules when the message/call was received in Austria. However, it is often not possible for the authority to prosecute legal violations abroad.

9.4 Is/are the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?

The competent authority for the enforcement of section 107 TKG is the Telecommunications Authority (Fernmeldebüro); the data protection authority is not responsible for the enforcement of such violations. The Fernmeldebüro mainly becomes active when somebody makes a complaint.

9.5 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?

Undertakings holding a licence under section 151 Trade, Commerce and Industry Regulation Act (Gewerbeordnung) are entitled to collect (non-sensitive) data from publicly available sources (and to add classifications for specific marketing purposes) for the preparation and execution of marketing purposes for third parties. Furthermore, these undertakings are entitled to sell such lists to third parties and to act as an intermediary between the owners and users of marketing lists. The use of data contained in marketing lists of third parties without the consent of the data subjects is only possible for certain data (essentially name, address, date of birth, profession) and if the owner of the marketing lists declares in writing that the data subjects have been informed about the possibility to prohibit the transfer for marketing purposes of third parties, and have not pronounced such prohibition. The collection of any sensitive data requires the explicit consent of the data subject. Furthermore, when using purchased marketing lists from third parties for the purpose of sending any electronic communication, it needs to be safeguarded that the recipient of the advertising has indeed given consent for electronic direct marketing.

10 Cookies

10.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).

Section 96 para 3 TKG implements Article 5 of the EU ePrivacy Directive. Pursuant to Article 5 of the EU ePrivacy Directive, the storage of cookies (or other data) on an end user’s device requires prior consent (the applicable standard of consent is derived from the GDPR and before 25 May 2018 from Directive 95/46/EC). For the requirements of valid consent, compare the respective definition in section 2 above. This does not apply if: (i) the cookie is for the sole purpose of carrying out the transmission of a communication over an electronic communications network; or (ii) the cookie is strictly necessary to provide an “information society service” (e.g., a service over the internet) requested by the subscriber or user, which means that it must be essential to fulfill their request.

10.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?

The WP29 published Working Document 02/2013 (WP 208), which provides guidance on obtaining consent for cookies. Following WP29, the consent to the use of cookies containing personal data has to be explicit opt-in consent. The opinion of WP29 is not legally binding but it is usually used by the relevant authorities to determine the content of data protection legislation; in this case, section 96 para 3 TKG and the necessary consent.

As outlined in question 10.1 above, section 96 para 3 TKG distinguishes between: cookies serving the sole purpose of carrying out the transmission of a communication via an electronic communications network or necessary to provide an “information society service” requested by the subscriber or user (which do not require the consent of the user); and any other cookies.

10.3 To date, have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?

We are not aware of any publicly known enforcement action in this respect.
10.4 What are the maximum penalties for breaches of applicable cookie restrictions?

An infringement of section 96 para 3 TKG constitutes an administrative offence that is punishable by a fine of up to EUR 37,000.

11 Restrictions on International Data Transfers

11.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.

Data transfers to other jurisdictions that are not within the European Economic Area (“EEA”) can only take place if the transfer is to an “Adequate Jurisdiction” (as specified by the EU Commission) or the business has implemented one of the required safeguards as specified by the GDPR. The EU Commission has issued decisions concerning an adequate level of protection for the following countries: Andorra; Argentina; Canada; Faroe Islands; Guernsey; Isle of Man; Israel; Jersey; New Zealand; Switzerland; and Uruguay.

11.2 Please describe the mechanisms businesses typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract, data subject’s legitimate interest, etc.).

When transferring personal data to a country other than an Adequate Jurisdiction, businesses must ensure that there are appropriate safeguards on the data transfer, as prescribed by the GDPR. The GDPR offers a number of ways to ensure compliance for international data transfers, one of which is via the consent of the relevant data subject. Other common options are the use of Standard Contractual Clauses (“SCCs”) or Binding Corporate Rules (“BCRs”). Businesses can adopt the SCCs drafted by the EU Commission – these are available for transfers among controllers, and transfers between a controller (as exporter) and a processor (as importer). International data transfers may also take place based on contracts agreed between the data exporter and data importer provided that they meet the protection standards outlined in the GDPR, and they have prior approval by the relevant data protection authority.

International data transfers within a group of businesses can be safeguarded by the implementation of BCRs. The BCRs will always need approval from the relevant data protection authority. Most importantly, the BCRs will need to include a mechanism to ensure they are legally binding and enforced by every member in the group of businesses. Among other things, the BCRs must set out the group structure of the businesses, the proposed data transfers and their purpose, the rights of data subjects, the mechanisms that will be implemented to ensure compliance with the GDPR and the relevant compliant procedures.

Transfer of personal data to the US is also possible if the data importer has signed up to the EU-US Privacy Shield Framework, which was designed by the US Department of Commerce and the EU Commission to provide businesses in the EU and the US with a mechanism to comply with data protection requirements when transferring personal data from the EU to the US.

11.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.

It is likely that the international data transfer will require prior approval from the relevant data protection authority unless they have already established a GDPR-compliant mechanism, as set out above, for such transfers.

In any case, most of the safeguards outlined in the GDPR will need initial approval from the data protection authority, such as the establishment of BCRs.

12 Whistle-blower Hotlines

12.1 What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?

Internal whistle-blowing schemes are generally established in pursuance of a concern to implement proper corporate governance principles in the daily functioning of businesses. Whistle-blowing is designed as an additional mechanism for employees to report misconduct internally through a specific channel, and supplements a business’s regular information and reporting channels, such as employee representatives, line management, quality-control personnel or internal auditors who are employed precisely to report such misconduct.

The WP29 has limited its Opinion 1/2006 on the application of EU data protection rules to internal whistle-blowing schemes to the fields of accounting, internal accounting controls, auditing matters, the fight against bribery, banking and financial crime. The scope of corporate whistle-blower hotlines, however, does not need to be limited to any particular issues. The WP29 recommends that the business responsible for the whistle-blowing scheme should carefully assess whether it might be appropriate to limit the number of persons eligible for reporting alleged misconduct through the whistle-blowing scheme and whether it might be appropriate to limit the number of persons who may be reported through the scheme, particularly in the light of the seriousness of the alleged offences reported.

Prior to the entry into force of the GDPR, the DSG issued several permits for whistle-blowing schemes subject to a set of conditions detailing the required procedural safeguards and the design of such systems (e.g., confidentiality with regard to the whistle-blower, access to accusation for the person concerned, deletion of data after the cessation of investigations). Although the pre-approval requirements do not apply any more, the authority will likely continue to apply these principles in an ex post control.

Notably, Article 10 GDPR requires that the processing of personal data relating to criminal convictions and offences shall only be carried out under the control of an official authority or when the processing is authorised by EU or a Member State’s law. In Austria, the now amended section 4 para 3 DSG provides for the processing of personal data relating to criminal offences (including suspicions about such offences), if such processing is necessary to safeguard
12.2 Is anonymous reporting prohibited, strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do businesses typically address this issue?

Anonymous reporting is not prohibited under EU data protection law; however, it raises problems considering the essential requirement that personal data should only be collected fairly. As a rule, the WP29 considers that only identified reports should be advertised in order to satisfy this requirement. Businesses should not encourage or advertise the fact that anonymous reports may be made through a whistle-blower scheme.

Similarly the DSB, in its formerly issued permits, stipulated that businesses implementing such schemes should not encourage anonymous reporting, but had to assure full confidentiality for anonymous whistle-blowers.

An individual who intends to report to a whistle-blowing system should be aware that he/she will not suffer reprisal due to his/her action. The whistle-blower, at the time of establishing the first contact with the scheme, should be informed that his/her identity will be kept confidential at all the stages of the process and, in particular, will not be disclosed to third parties, such as the incriminated person, or to the employee’s line management. If, despite this information, the person reporting to the scheme still wants to remain anonymous, the report will be accepted into the scheme. Whistle-blowers should be informed that their identity might need to be disclosed to the relevant people involved in any further investigation or subsequent judicial proceedings instigated because of any enquiry conducted by the whistle-blowing scheme.

13 CCTV

13.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?

The use of CCTV is allowed if made in accordance with sections 12, 13 DSG. In such case, no DPIA must be undertaken in line with Article 35 para 10 GDPR. Sections 12 and 13 DSG have been enacted in accordance with Article 6 para 2 and 3, Article 23 and chapter IX GDPR and following the experience gained in practice under the rules on CCTV that were contained in the DSG 2000.

In principle, CCTV is allowed if:

- it is required in the vital interests of a person;
- the data subject has consented to the use of its data;
- it is allowed by specific legal provisions; or
- in case of preponderant legal interests of the controller or a third person, provided that the processing is proportionate.

Section 12 para 3 DSG specifies that preponderant legal interests are given in case the CCTV is made for purposes of:

- the precautionary protection of persons or things on private property that is used only by the controller;
- the precautionary protection of persons or things on publicly accessible property being under the domestic authority of the controller, in case violations have already happened in the past or there is a specific potential danger; or
- a private documentation interest in case the CCTV is directed neither to capture uninvolved persons in a way which allows their identification, nor to capture objects which would indirectly allow the identification of such persons.

In principle, CCTV needs to be specifically marked by a sign which identifies the respective controller (section 13 para 5 DSG). Moreover, any processing, except real-time surveillance, has to be logged (section 13 para 2 DSG).

The DSB has stated in its White List for the DPIA that specific CCTV processing (as defined in the White List) does not require a DPIA.

13.2 Are there limits on the purposes for which CCTV data may be used?

According to section 12 para 4 DSG, CCTV is not permitted for the purpose of: (i) recordings of persons in their strictly personal spheres of life (please see question 14.1 below); (ii) control of employees in the workplace (please see question 14.1 below); (iii) automation-supported comparison of personal data obtained by means of CCTV without consent or for personal profiling with other personal data; and (iv) the evaluation of personal data obtained by means of CCTV on the basis of special categories of personal data (Article 9 GDPR) as a selection criterion.

Section 13 para 3 DSG provides that any recordings of personal data have to be deleted if they are no longer required for the purpose for which they were collected, unless another legal obligation applies. In any case, the storing of recordings exceeding 72 hours needs to be proportionate and needs to be separately documented and justified.

14 Employee Monitoring

14.1 What types of employee monitoring are permitted (if any), and in what circumstances?

Section 12 para 4 subparagraph 1 DSG provides that CCTV is prohibited at locations that are deemed to be part of the most personal areas of the data subject’s life (e.g., their homes in general and also changing rooms, bathrooms, etc.) without explicit consent. Furthermore, CCTV for the purpose of control of employees in the workplace (efficiency control) is expressly prohibited (section 12 para 4 subparagraph 2 DSG).

This provision does not generally prevent the surveillance of workplaces (e.g., the surveillance of dangerous machines in order to protect the employees or the surveillance of, e.g., the counter hall of a bank), as long as the purpose is not efficiency control or employee monitoring as such. In most cases of video surveillance of a workplace, the works council will need to give its consent to such surveillance. Furthermore, please refer to the answers to section 13 above.

14.2 Is consent or notice required? Describe how employers typically obtain consent or provide notice.

Pursuant to section 13 para 5 DSG, CCTV must be marked appropriately.
If a works council is established in the respective entity, an agreement needs to be concluded with the works council. Individual consent of the employee does not suffice in this case. If no works council is established, each employee needs to provide its consent to the respective video surveillance of its workplace (if such is not already prohibited by section 12 para 4 subparagraph 2 DSG).

14.3 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?

Please see question 14.2 above.

15 Data Security and Data Breach

15.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?

Yes. Personal data must be processed in a way that ensures security and safeguards against unauthorised or unlawful processing, accidental loss, destruction and damage of the data.

Both controllers and processors must ensure they have appropriate technical and organisational measures in place to meet the requirements of the GDPR. Depending on the security risk as well as the nature, scope and purpose of the processing activities, this may include: the encryption or pseudonymisation of personal data; the ability to ensure the ongoing confidentiality, integrity and resilience of processing systems; an ability to restore access to data following a technical or physical incident; and a process for regularly testing and evaluating the technical and organisational measures for ensuring the security of processing.

15.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

The controller is responsible for reporting a personal data breach without undue delay (and in any case within 72 hours of first becoming aware of the breach) to the relevant data protection authority, unless the breach is unlikely to result in a risk to the rights and freedoms of the data subject(s). A processor must notify any data breach to the controller without undue delay.

The notification must include the nature of the personal data breach including the categories and number of data subjects concerned, the name and contact details of the Data Protection Officer or relevant point of contact, the likely consequences of the breach and the measures taken to address the breach, including attempts to mitigate possible adverse effects.

15.3 Is there a legal requirement to report data breaches to affected data subjects? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

Controllers have a legal obligation to communicate the breach to the data subject without undue delay, if the breach is likely to result in a high risk to the rights and freedoms of the natural persons. If the controller is in default with such obligation, the competent authority may require the controller to inform the data subject.

The notification must include the description of the breach, name and contact details of the Data Protection Officer (or point of contact), the likely consequences of the breach, any measures taken to remedy or mitigate the breach and recommendations to mitigate potential consequences.

The controller may be exempt from notifying the data subject if the risk of harm is remote (e.g., because the affected data is encrypted), the controller has taken measures to minimise the risk of harm (e.g., suspending affected accounts) or the notification requires a disproportionate effort (e.g., a public notice of the breach).

The WP29 has issued guidelines on the data breach notification detailing requirements for data breach notifications (WP 250).

15.4 What are the maximum penalties for data security breaches?

The maximum penalty is the higher of EUR 20 million or 4% of worldwide turnover.

16 Enforcement and Sanctions

16.1 Describe the enforcement powers of the data protection authority(ies).

<table>
<thead>
<tr>
<th>Investigatory Power</th>
<th>Civil/Administrative Sanction</th>
<th>Criminal Sanction</th>
</tr>
</thead>
<tbody>
<tr>
<td>Investigative Powers</td>
<td>The data protection authority has wide powers to order the controller and the processor to provide any information it requires for the performance of its tasks, to conduct investigations in the form of data protection audits, to carry out reviews on certificates issued pursuant to the GDPR, to notify the controller or processor of alleged infringement of the GDPR, to access all personal data and all information necessary for the performance of controllers’ or processors’ tasks and access to the premises of the data including any data processing equipment.</td>
<td>N/A</td>
</tr>
</tbody>
</table>

© Published and reproduced with kind permission by Global Legal Group Ltd, London
The data protection authority has a wide range of powers to advise the controller, accredit certification bodies and to authorise certificates, contractual clauses, administrative arrangements and binding corporate rules as outlined in the GDPR.

The GDPR provides for administrative fines which can be EUR 20 million or up to 4% of the business’s worldwide annual turnover of the proceeding financial year. The DSG contains further administrative fines – subsidiary to the GDPR fines – of up to EUR 50,000.

The GDPR provides for administrative fines which will be EUR 20 million or up to 4% of the business’s worldwide annual turnover of the proceeding financial year, whichever is higher.

16.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?

The GDPR entitles the relevant data protection authority – in Austria the DSB – to impose a temporary or definitive limitation including a ban on processing. Such ban can be imposed by the DSB by rendering a decision (Bescheid); no court order is required.

16.3 Describe the data protection authority’s approach to exercising those powers, with examples of recent cases.

Since the GDPR came into force, the DSB has not exercised the respective powers. However, the authority has issued bans under the old data protection regime in the past.

16.4 Does the data protection authority ever exercise its powers against businesses established in other jurisdictions? If so, how is this enforced?

Since the GDPR came into force, the DSB has – as far as we are aware based on publicly available information – not exercised its powers against businesses established in other jurisdictions.

17 E-discovery / Disclosure to Foreign Law Enforcement Agencies

17.1 How do businesses typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?

Austrian law does not contain an equivalent to discovery or e-discovery as known in US law. Foreign e-discovery requests will generally collide with data protection law, as the normal rules will apply as to whether it is permitted to transfer data a) to a third party or b) to a country outside the EEA which does not provide for adequate data protection.

17.2 What guidance has/have the data protection authority(ies) issued?

The DSB has so far not issued any guidance in this respect.

18 Trends and Developments

18.1 What enforcement trends have emerged during the previous 12 months? Describe any relevant case law.

The DSB began to apply the GDPR in its decisions and to enforce the rights of data subjects thereunder. With these initial rulings, the DSB in part clarified its approach to and interpretation of several provisions of the regulation.

The most noteworthy decisions so far concerned the right to erasure provisions of the regulation. The DSB has so far not issued any guidance in this respect.
website, who claimed a violation of his right to withdraw consent. The website in question could be used either with a fee-based subscription without any cookies, or free of charge but with the requirement of consent to the use of cookies. The DSB ruled that the user was offered a free choice between the two options, and that the consequences of the non-provision of consent (i.e. the subscription or the use of another medium of information) did not constitute a substantial disadvantage for the data subject.

Until March 2019, the DSG imposed fines for violations of the GDPR in only five cases; all these cases concerned prohibited video surveillance. In many other cases, the DSB has issued warnings.

18.2 What “hot topics” are currently a focus for the data protection regulator?

Austria had earlier enacted an “implementation act” to the GDPR. With the subsequent Data Protection Deregulation Act 2018 (BGBl. I 24/2018), which attracted a lot of public and scientific attention, the Austrian legislature intended to ease the compliance requirements with regard to data protection for businesses. Section 11 DSG requires the data protection authority to respect the principle of proportionality in imposing fines pursuant to Article 83 GDPR. The authority primarily has to apply remedies such as issuing warnings instead of imposing fines, in case of first-time violations. In addition, section 4 para 6 DSG now limits the right to information of the data subject in cases where trade or business secrets of the controller are affected. This act raised the concern that the legislature might neutralise the strict approach of the GDPR. Although another amendment of the DSG has been enacted (BGBl. I Nr. 14/2019), the intended limitation of the personal scope of application of the constitutional right to data protection, again, was not achieved. Therefore, the Austrian constitutional right to data protection continues to refer not only to natural persons, but also to legal entities.

Furthermore, the DSB has issued a Whitelist as well as a Blacklist in 2018, detailing the exemptions and, conversely, the unconditional obligations for conducting DPIAs in Austria. As for the European legislation, it may be expected that the Commission will publish implementation guidelines and provisions where necessary. Among other important issues, adapted standard contractual clauses for the transfer of personal data to third countries could be decided upon in the near future. Moreover, the proposal for a new E-Privacy Directive is still pending in the legislative process (see Procedure File 2017/0003/COD).
Chapter 8

Belgium

Lydian Bastiaan Bruyndonckx
Olivia Santantonio

1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

Since 25 May 2018, the principal data protection legislation in the EU has been Regulation (EU) 2016/679 (the “General Data Protection Regulation” or “GDPR”). The GDPR repealed Directive 95/46/EC (the “Data Protection Directive”) and has led to increased (though not total) harmonisation of data protection law across the EU Member States.

1.2 Is there any other general legislation that impacts data protection?

The law of 13 June 2005 on electronic communications implements the requirements of Directive 2002/58/EC (as amended by Directive 2009/136/EC) (the “ePrivacy Directive”), which provides a specific set of privacy rules to harmonise the processing of personal data by the telecoms sector. In January 2017, the European Commission published a proposal for an ePrivacy regulation (the “ePrivacy Regulation”) that would harmonise the applicable rules across the EU and replace the current ePrivacy Directive (and its implementing national legislation). In September 2018, the Council of the European Union published proposed revisions to the draft. The ePrivacy Regulation is still in draft form at this stage and it is unclear when it will be finalised.

In addition, the Belgian legislator has adopted secondary legislation pursuant to the GDPR.

The law of 3 December 2017 on the establishment of the Data Protection Authority implements the requirements of the GDPR with respect to national supervisory authorities, and reforms the Belgian Commission for the Protection of Privacy. As of 25 May 2018, the Belgian Commission for the Protection of Privacy carries the name “Data Protection Authority” and has the powers and competences which the GDPR requires national supervisory authorities to possess.

A second act, the law of 30 July 2018 on the protection of individuals with respect to the processing of personal data (the “GDPR Implementation Act”), addresses the national substantive aspects of the GDPR and introduces several specifications and derogations, such as determining the age of consent for children in an online context and imposing additional security measures in relation to sensitive data. At the same time, it abolishes and replaces the 1992 Data Protection Act and the 2001 Royal Decree which implemented it.

1.3 Is there any sector-specific legislation that impacts data protection?

Book XII of the Code of Economic Law, which deals with certain legal aspects of information society services, provides a specific set of rules regarding the use of personal data for direct marketing purposes via electronic post, which includes email, SMS and MMS. Books VI and XIV of the Code of Economic Law, which deal with market practices and consumer protection, provide a specific set of rules regarding the use of personal data for direct marketing purposes via telephone, fax and automatic calling machines without human intervention.

The Law of 3 August 2012 contains provisions relating to the processing of personal data carried out by the Federal Public Service – Finance in the framework of the carrying out of its mission. The Flemish Decree of 18 July 2008 provides a specific set of rules concerning the exchange of administrative data by regional authorities within the Flemish region.

1.4 What authority(ies) are responsible for data protection?

Since 25 May 2018, the former Commission for the Protection of Privacy carries the name “Data Protection Authority” and has the powers and competences which the GDPR requires national supervisory authorities to possess.

2 Definitions

2.1 Please provide the key definitions used in the relevant legislation:

- “Personal Data” means any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
- “Processing” means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by
transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

- “Controller” means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
- “Processor” means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
- “Data Subject” means an individual who is the subject of the relevant personal data.
- “Sensitive Personal Data” are personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, data concerning health or sex life and sexual orientation, genetic data or biometric data.
- “Data Breach” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.
- “Personal Data relating to Criminal Convictions” are personal data relating to criminal convictions and offences or related security measures.

3 Territorial Scope

3.1 Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to those laws?

The GDPR applies to businesses that are established in any EU Member State and that process personal data (either as a controller or processor, and regardless of whether or not the processing takes place in the EU) in the context of that establishment.

A business that is not established in any Member State but is subject to the laws of a Member State by virtue of public international law is also subject to the GDPR.

The GDPR applies to businesses outside the EU if they (either as a controller or processor) process the personal data of EU residents in relation to: (i) the offering of goods or services (whether or not in return for payment) to EU residents; or (ii) the monitoring of the behaviour of EU residents (to the extent that such behaviour takes place in the EU).

4 Key Principles

4.1 What are the key principles that apply to the processing of personal data?

- Transparency
  Personal data must be processed lawfully, fairly and in a transparent manner. Controllers must provide certain minimum information to data subjects regarding the collection and further processing of their personal data. Such information must be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

- Lawful basis for processing
  Processing of personal data is lawful only if, and to the extent that, it is permitted under EU data protection law. The GDPR provides an exhaustive list of legal bases on which personal data may be processed, of which the following are the most relevant for businesses: (i) prior, freely given, specific, informed and unambiguous consent of the data subject; (ii) contractual necessity (i.e., the processing is necessary for the performance of a contract to which the data subject is a party, or for the purposes of pre-contractual measures taken at the data subject’s request); (iii) compliance with legal obligations (i.e., the controller has a legal obligation, under the laws of the EU or an EU Member State, to perform the relevant processing); or (iv) legitimate interests (i.e., the processing is necessary for the purposes of legitimate interests pursued by the controller, except where the controller’s interests are overridden by the interests, fundamental rights or freedoms of the affected data subjects).

Please note that businesses require stronger grounds to process sensitive personal data. The processing of sensitive personal data is only permitted under certain conditions, of which the most relevant for businesses are: (i) explicit consent of the affected data subject; (ii) the processing is necessary in the context of employment law; or (iii) the processing is necessary for the establishment, exercise or defence of legal claims.

- Purpose limitation
  Personal data may only be collected for specified, explicit and legitimate purposes and must not be further processed in a manner that is incompatible with those purposes. If a controller wishes to use the relevant personal data in a manner that is incompatible with the purposes for which they were initially collected, it must: (i) inform the data subject of such new processing; and (ii) be able to rely on a lawful basis as set out above.

- Data minimisation
  Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which those data are processed. A business should only process the personal data that it actually needs to process in order to achieve its processing purposes.

- Accuracy
  Personal data must be accurate and, where necessary, kept up to date. A business must take every reasonable step to ensure that personal data that are inaccurate are either erased or rectified without delay.

- Retention
  Personal data must be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

- Data security
  Personal data must be processed in a manner that ensures appropriate security of those data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

- Accountability
  The controller is responsible for, and must be able to demonstrate, compliance with the data protection principles set out above.

5 Individual Rights

5.1 What are the key rights that individuals have in relation to the processing of their personal data?

- Right of access to data/copies of data
  A data subject has the right to obtain from a controller the following information in respect of the data subject’s personal data: (i) confirmation of whether, and where, the controller is processing the data subject’s personal data; (ii) information about the purposes of the processing; (iii)
What are the sanctions for failure to register/notify? Is there a legal obligation on businesses to register with or notify the data protection authority? Who must register with or notify the data protection authority? Belgium

Right to rectification of errors Controllers must ensure that inaccurate or incomplete data are erased or rectified. Data subjects have the right to rectification of inaccurate personal data.

Right to deletion/right to be forgotten Data subjects have the right to erasure of their personal data (the “right to be forgotten”) if: (i) the data are no longer needed for their original purpose (and no new lawful purpose exists); (ii) the lawful basis for the processing is the data subject’s consent, the data subject withdraws that consent, and no other lawful ground exists; (iii) the data subject exercises the right to object, and the controller has no overriding grounds for continuing the processing; (iv) the data have been processed unlawfully; or (v) erasure is necessary for compliance with EU law or national data protection law.

Right to object to processing Data subjects have the right to object, on grounds relating to their particular situation, to the processing of personal data where the basis for that processing is either public interest or legitimate interest of the controller. The controller must cease such processing unless it demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the relevant data subject or requires the data in order to establish, exercise or defend legal rights.

Right to restrict processing Data subjects have the right to restrict the processing of personal data, which means that the data may only be held by the controller, and may only be used for limited purposes if: (i) the accuracy of the data is contested and only for as long as it takes to verify that accuracy; (ii) the processing is unlawful and the data subject requests restriction (as opposed to exercising the right to erasure); (iii) the controller no longer needs the data for their original purpose, but the data are still required by the controller to establish, exercise or defend legal rights; or (iv) verification of overriding grounds is pending, in the context of an erasure request.

Right to data portability Data subjects have a right to receive a copy of their personal data in a commonly used machine-readable format and transfer their personal data from one controller to another or have the data transmitted directly between controllers.

Right to withdraw consent A data subject has the right to withdraw his/her consent at any time. The withdrawal of consent does not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject must be informed of the right to withdraw consent. It must be as easy to withdraw consent as to give it.

Right to object to marketing Data subjects have the right to object to the processing of personal data for the purpose of direct marketing, including profiling.

6 Registration Formalities and Prior Approval

6.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?

No, the obligation to notify the Data Protection Authority of any wholly or partially automated processing of personal data, which existed prior to the entry into force of the GDPR, has been abolished as of the entry into force of the GDPR on 25 May 2018.

6.2 If such registration/notice is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?

This is not applicable in our jurisdiction.

6.3 On what basis are registrations/notifications made (e.g., per legal entity, per processing purpose, per data category, per system or database)?

This is not applicable in our jurisdiction.

6.4 Who must register with/notify the data protection authority (e.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation)?

This is not applicable in our jurisdiction.

6.5 What information must be included in the registration/notice (e.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes)?

This is not applicable in our jurisdiction.

6.6 What are the sanctions for failure to register/notify where required?

This is not applicable in our jurisdiction.
7.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect of his or her role as a Data Protection Officer?

The appointed Data Protection Officer should not be dismissed or penalised for performing his/her tasks and should report directly to the highest management level of the controller or processor.

7.4 Can a business appoint a single Data Protection Officer to cover multiple entities?

A single Data Protection Officer is permitted by a group of undertakings provided that the Data Protection Officer is easily accessible from each establishment.

7.5 Please describe any specific qualifications for the Data Protection Officer required by law.

The Data Protection Officer should be appointed on the basis of professional qualities and should have an expert knowledge of data protection law and practices. While this is not strictly defined, it is clear that the level of expertise required will depend on the circumstances. For example, the involvement of large volumes of sensitive personal data will require a higher level of knowledge.

7.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?

The Data Protection Officer should be involved in all issues which relate to the protection of personal data. The GDPR outlines the minimum tasks required by the Data Protection Officer, which include: (i) informing the controller, processor and their relevant employees who process data of their obligations under the GDPR; (ii) monitoring compliance with the GDPR, national data protection legislation and internal policies in relation to the processing of personal data including internal audits; (iii) advising on data protection impact assessments (“DPIAs”) and the training of staff; and (iv) co-operating with the Data Protection Authority and acting as the authority’s primary contact point for issues related to data processing.

7.7 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?

Yes, the controller or processor must notify the Data Protection Authority of the contact details of the designated Data Protection Officer.

7.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?

The Data Protection Officer does not necessarily need to be named in the public-facing privacy notice. However, the contact details of the Data Protection Officer must be notified to the data subject when personal data relating to that data subject are collected. As a matter of good practice, the Article 29 Working Party (the “WP29”) recommended in its 2017 guidance on Data Protection Officers that both the Data Protection Authority and employees should be notified of the name and contact details of the Data Protection Officer.

6.7 What is the fee per registration/notification (if applicable)?

This is not applicable in our jurisdiction.

6.8 How frequently must registrations/notifications be renewed (if applicable)?

This is not applicable in our jurisdiction.

6.9 Is any prior approval required from the data protection regulator?

Prior approval of the Data Protection Authority is required for transfers outside the European Economic Area to a country not offering adequate protection of personal data and that are based upon bespoke contractual safeguards rather than Standard Contractual Clauses approved by the EU Commission.

6.10 Can the registration/notification be completed online?

This is not applicable in our jurisdiction.

6.11 Is there a publicly available list of completed registrations/notifications?

This is not applicable in our jurisdiction.

6.12 How long does a typical registration/notification process take?

This is not applicable in our jurisdiction.

7 Appointment of a Data Protection Officer

7.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.

The appointment of a Data Protection Officer for controllers or processors is only mandatory in some circumstances, including where there is: (i) large-scale regular and systematic monitoring of individuals; (ii) large-scale processing of sensitive personal data; or (iii) processing carried out by a public authority or body, except in the exercise of judicial functions by courts.

The Belgian legislator has not adopted secondary legislation which renders the appointment of a Data Protection Officer mandatory in cases other than those described in the GDPR.

Where a business designates a Data Protection Officer voluntarily, the requirements of the GDPR apply as though the appointment were mandatory.

7.2 What are the sanctions for failing to appoint a Data Protection Officer where required?

In the circumstances where the appointment of a Data Protection Officer is mandatory, failure to comply may result in the wide range of penalties available under the GDPR, including administrative fines.
8 Appointment of Processors

8.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?

Yes, the business that appoints a processor to process personal data on its behalf is required to enter into an agreement with the processor which sets out the subject matter for processing, the duration of processing, the nature and purpose of processing, the types of personal data and categories of data subjects and the obligations and rights of the controller (i.e., the business).

It is essential that the processor appointed by the business complies with the GDPR.

8.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?

The processor must be appointed under a binding agreement or other legal act in writing, including in electronic form. The contractual terms must stipulate that the processor: (i) only acts on the documented instructions of the controller; (ii) imposes confidentiality obligations on all employees; (iii) ensures the security of personal data that it processes; (iv) abides by the rules regarding the appointment of sub-processors; (v) implements measures to assist the controller with guaranteeing the rights of data subjects; (vi) assists the controller in carrying out DPIAs and obtaining approval from the Data Protection Authority, where required; (vii) either returns or destroys the personal data at the end of the relationship (except as required by EU or Member State law); and (viii) provides the controller with all the information necessary to demonstrate compliance with the GDPR, and allows for and contributes to audits, including inspections, conducted by the controller or another auditor mandated by the controller.

9 Marketing

9.1 Please describe any legislative restrictions on the sending of electronic direct marketing (e.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?).

Direct marketing per electronic post (which includes email, SMS and MMS) is only authorised where the recipient specifically and freely consented to it (opt-in). However, there are two exceptions to this rule. Firstly, sending electronic direct marketing to legal entities using a non-personal email address (e.g., info@company.com) is allowed on an opt-out basis. Secondly, sending electronic direct marketing to existing customers about identical or similar products is also allowed on an opt-out basis, provided a number of strict conditions are met. It should be noted that, even when the recipient previously consented to the use of his/her electronic contact details for direct marketing purposes, he/she can at any time oppose the further use of his/her electronic contact details for direct marketing purposes.

9.2 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.).

For marketing by telephone, a national opt-out register (the so-called “Robinson List”) exists and businesses carrying out direct marketing by telephone are required to check this list in advance.

Direct marketing by post does not require the prior consent of the addressee but can be carried out on an opt-out basis. For direct marketing (on a personalised basis) by post, a national opt-out register has been put in place but is only mandatory for businesses that are members of the Belgian Direct Marketing Association (“BDMA”).

For non-personalised advertising by post, anyone can ask to be provided with “Stop-Pub” stickers to stick on his/her mailbox.

For marketing by fax or via automated calling machines without human intervention, the prior consent of the recipient is required (opt-in).

9.3 Do the restrictions noted above apply to marketing sent from other jurisdictions?

Yes, they do.

9.4 Is/are the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?

Under the GDPR, the Data Protection Authority will have the right to carry out investigations and enforce the GDPR, including by imposing administrative sanctions. Aside from the Data Protection Authority, the Economic Inspection (which is part of the Federal Public Service Economy) has powers to enforce the specific rules on direct marketing which form part of Books VI, XII and XIV of the Code of Economic Law. Both authorities are active in enforcement of breaches of marketing restrictions. Most investigations are, however, started on the basis of complaints filed by individuals.

9.5 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?

Yes, provided that data protection legislation is complied with. This means, amongst others, that the collection and processing of the data must have been carried out in compliance with the principles of the GDPR (including lawful basis, compliance with the opt-in and opt-out rules, transparency, purpose limitation, accuracy, security and confidentiality).

Businesses are strongly advised to seek appropriate guarantees from the seller of marketing lists, including with respect to (i) the fact that the data have been gathered and processed in compliance with the GDPR, (ii) the fact that the individuals whose data are included have consented to the use of their data for direct marketing purposes, and (iii) the fact that the transfer of the data is in accordance with the fair processing notices provided to the individuals and with the GDPR.

9.6 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?

The maximum penalty for sending marketing communications in breach of applicable restrictions is a criminal fine of EUR 10,000.
This amount is to be multiplied by eight in accordance with the law on criminal surcharges.

10 Cookies

10.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).

The Law of 13 June 2005 on electronic communications implements Article 5 of the ePrivacy Directive. Pursuant to Article 5 of the EU ePrivacy Directive, the storage of cookies (or other data) on an end user’s device requires prior consent (the applicable standard of consent is derived from the GDPR). For consent to be valid, it must be informed, specific, freely given and must constitute a real and unambiguous indication of the individual’s wishes. This does not apply if: (i) the cookie is for the sole purpose of carrying out the transmission of a communication over an electronic communications network; or (ii) the cookie is strictly necessary to provide an “information society service” (i.e., a service provided over the internet) requested by the subscriber or user, which means that it must be essential to fulfil the user’s request.

The use of cookies is only authorised if the person has had, before any use of cookies, clear and precise information concerning the purpose of the processing and his rights. The controller must also freely give the opportunity to the subscriber or users to withdraw their consent at any time. Information must also be provided with respect to the term of validity of the cookies used.

The EU Commission intends to pass a new ePrivacy Regulation that will replace the respective national legislation in the EU Member States. The ePrivacy Regulation is planned to come into force in 2019.

10.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?

The applicable restrictions indeed distinguish between different types of cookies. A distinction is made, amongst others, between session cookies (which have a time limit and are deleted after the browsing session) and permanent cookies (which are kept on the user’s hard drive for an indefinite duration). Furthermore, a distinction is made between first-party cookies (which are placed by the website owner) and third-party cookies (which are placed by a third party, e.g., Facebook or Google). A distinction is also made between tracking cookies (which are used to collect data about the browsing behaviour of the user on various websites) and other cookies. In principle, the storage of cookies on an end user’s device requires prior consent. This does not, however, apply to merely technical cookies and necessary cookies.

10.3 To date, has/have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?

The Belgian Institute of Postal Services and Telecommunications (“BIPT/IBPT”) is in charge of monitoring compliance by businesses with the Law of 13 June 2005 on electronic communications, together with the Data Protection Authority. In 2017, the Commission for the Protection of Privacy (being the predecessor of the Data Protection Authority) took aim at Facebook in connection with the use of cookies for the purposes of tracking internet users and instituted proceedings against Facebook in connection therewith. By a decision dated 16 February 2018, Facebook was condemned by the Brussels Court of First Instance for having tracked an internet user without them either knowing or consenting. The court issued a fine of EUR 250,000 per day with a maximum fine of EUR 100,000,000. Other than the high-profile Facebook case mentioned above, we are not aware of other enforcement actions having been taken by the Commission for the Protection of Privacy specifically in relation to cookies.

10.4 What are the maximum penalties for breaches of applicable cookie restrictions?

There are no specific (criminal) sanctions linked to the breach of the applicable cookie restrictions as laid down in the Law of 13 June 2005 on electronic communications. To the extent the breach also constitutes a breach of the applicable data protection laws (e.g., the obligation to inform the data subject of the processing of personal data), the controller could, however, be sanctioned with criminal fines applicable for breaches of the data protection laws. Under the current legislation based upon the Data Protection Directive, a breach of the data protection legislation can give rise to criminal fines of up to EUR 100,000. This amount is to be multiplied by eight in accordance with the law on criminal surcharges.

11 Restrictions on International Data Transfers

11.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.

Data transfers to other jurisdictions that are not within the European Economic Area (the “EEA”) can only take place if the transfer is to an “Adequate Jurisdiction” (as specified by the EU Commission) or the business has implemented one of the required safeguards as specified by the GDPR, or one of the derogations specified in the GDPR applies to the relevant transfer. The EDPB Guidelines (2/2018) set out that a “layered approach” should be taken with respect to these transfer mechanisms. If the transfer is not to an Adequate Jurisdiction, the data exporter should first explore the possibility of implementing one of the safeguards provided for in the GDPR before relying on a derogation.

11.2 Please describe the mechanisms businesses typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).

When transferring personal data to a country other than an Adequate Jurisdiction, businesses must ensure that there are appropriate safeguards on the data transfer, as prescribed by the GDPR. The GDPR offers a number of ways to ensure compliance for international data transfers, of which one is consent of the relevant data subject. Other common options are the use of Standard Contractual Clauses or Binding Corporate Rules (“BCRs”).

Businesses can adopt the Standard Contractual Clauses drafted by the EU Commission – these are available for transfers between controllers, and transfers between a controller (as exporter) and a processor (as importer). International data transfers may also take place on the basis of contracts agreed between the data exporter and data importer provided that they conform to the protections outlined in the GDPR, and they have prior approval by the relevant data protection authority.
International data transfers within a group of businesses can be safeguarded by the implementation of BCRs. The BCRs will always need approval from the relevant data protection authority. Most importantly, the BCRs will need to include a mechanism to ensure they are legally binding and enforced by every member in the group of businesses. Among other things, the BCRs must set out the group structure of the businesses, the proposed data transfers and their purpose, the rights of data subjects, the mechanisms that will be implemented to ensure compliance with the GDPR and the relevant complaint procedures.

Transfer of personal data to the US is also possible if the data importer has signed up to the EU-US Privacy Shield Framework, which was designed by the US Department of Commerce and the EU Commission to provide businesses in the EU and the US with a mechanism to comply with data protection requirements when transferring personal data from the EU to the US.

11.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.

It is likely that the international data transfer will require prior approval from the relevant data protection authority unless they have already established a GDPR-compliant mechanism, as set out above, for such transfers.

In any case, most of the safeguards outlined in the GDPR will need initial approval from the Data Protection Authority, such as the establishment of BCRs.

12 Whistle-blower Hotlines

12.1 What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?

Internal whistle-blowing schemes are generally established in pursuance of a concern to implement proper corporate governance principles in the daily functioning of businesses. Whistle-blowing is designed as an additional mechanism for employees to report misconduct internally through a specific channel and supplements a business’ regular information and reporting channels, such as employee representatives, line management, quality-control personnel or internal auditors who are employed precisely to report such misconduct.

The WP29 has limited its Opinion 1/2006 on the application of EU data protection rules to internal whistle-blowing schemes to the fields of accounting, internal accounting controls, auditing matters, fight against bribery, banking and financial crime. The scope of corporate whistle-blower hotlines, however, does not need to be limited to any particular issues. In the Opinion, it is recommended that the business responsible for the whistle-blowing scheme should carefully assess whether it might be appropriate to limit the number of persons eligible for reporting alleged misconduct through the whistle-blowing scheme and whether it might be appropriate to limit the number of persons who may be reported through the scheme, in particular in the light of the seriousness of the alleged offences reported.

In 2007, the Commission for the Protection of Privacy also issued a recommendation on internal whistle-blowing schemes. The recommendation provides guidance to organisations on how to implement and operate whistle-blowing schemes in accordance with data protection law, and is largely inspired by the WP29 Opinion 1/2006 discussed above.

12.2 Is anonymous reporting prohibited, strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do businesses typically address this issue?

Anonymous reporting is not prohibited under EU data protection law; however, it raises problems as regards the essential requirement that personal data should only be collected fairly. In Opinion 1/2006, the WP29 considered that only identified reports should be advertised in order to satisfy this requirement. Businesses should not encourage or advertise the fact that anonymous reports may be made through a whistle-blower scheme.

An individual who intends to report to a whistle-blowing system should be aware that he/she will not suffer due to his/her action. The whistle-blower, at the time of establishing the first contact with the scheme, should be informed that his/her identity will be kept confidential at all the stages of the process, and in particular will not be disclosed to third parties, such as the incriminated person or to the employee’s line management. If, despite this information, the person reporting to the scheme still wants to remain anonymous, the report will be accepted into the scheme. Whistle-blowers should be informed that their identity may need to be disclosed to the relevant people involved in any further investigation or subsequent judicial proceedings instigated as a result of any enquiry conducted by the whistle-blowing scheme.

13 CCTV

13.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?

A DPIA must be undertaken with assistance from the Data Protection Officer when there is systematic monitoring of a publicly accessible area on a large scale. If the DPIA suggests that the processing would result in a high risk to the rights and freedoms of individuals prior to any action being taken by the controller, the controller must consult the Data Protection Authority.

During the course of a consultation, the controller must provide information on the responsibilities of the controller and/or processors involved, the purpose of the intended processing, a copy of the DPIA, the safeguards provided by the GDPR to protect the rights and freedoms of data subjects and, where applicable, the contact details of the Data Protection Officer.

If the Data Protection Authority is of the opinion that the CCTV monitoring would infringe the GDPR, it has to provide written advice to the controller within eight weeks of the request for a consultation, and can use any of its wider investigative, advisory and corrective powers outlined in the GDPR.

The Belgian legislator introduced a new administrative obligation in the Surveillance Camera Act as well as in the Police Service Act with regard to recording the use of cameras. This register forms an extensive logbook about the use of the cameras. Moreover, according to current Belgian legislation on surveillance cameras, installing
CCTV in public areas is only permitted after positive advice from the communal or city council and the chief of police, which requires a safety investigation. In addition, when installing CCTV in public areas, the controller must inform the local chief of police.

When installing CCTV, a sign must be placed to warn individuals that the area is under CCTV surveillance and to inform them of the identity and contact details of the controller.

13.2 Are there limits on the purposes for which CCTV data may be used?

CCTV for surveillance purposes can only be installed and used for the following purposes: (i) to prevent, record or detect offences; (ii) to prevent, record or detect disturbances; or (iii) to maintain public order.

CCTV can only be used in the workplace for the following purposes: (i) health and safety; (ii) protection of company property; (iii) surveillance of the production process; or (iv) monitoring of the work of employees. The employer must clearly and explicitly define the purposes of the CCTV system installed in the workplace.

14 Employee Monitoring

14.1 What types of employee monitoring are permitted (if any), and in what circumstances?

According to, amongst others, Collective Bargaining Agreement N° 68 (on the use of CCTV in the workplace) and Collective Bargaining Agreement N° 81 (on the monitoring of electronic communications in the workplace):

- the employer may monitor the hours worked through the use of a time registration system, but only if the employee has been informed of this use beforehand;
- the employer may consult the electronic agenda of an employee if it is necessary for the proper conduct of the business and there are no other, less intrusive, means to obtain the information;
- the employer may systematically monitor the professional telephone conversations in order to monitor the quality of the service, depending on the employee’s function; call centres must always inform their employees that the conversations may be recorded and listened to;
- emails of a professional nature may be accessed by the employer in the absence of the employee, in order to ensure the continuity of service, provided the employer complies with the data protection legislation; the employer must inform the employee beforehand that such access may happen and only look at the emails which seem to be related to ongoing cases and are related to the period in which the employee was absent without the correspondent knowing it;
- monitoring of electronic communications in the workplace is permitted to the extent the data protection laws and the Collective Bargaining Agreement N° 81 are complied with;
- the use of geo-localisation is permitted under strict conditions and only if there is no other, less intrusive, manner to monitor the employees; the data should not be kept longer than necessary; if the employer wishes to conduct an in-depth investigation, he must inform the employee and provide him the opportunity to be heard; and
- monitoring of employees through CCTV installed in the workplace is permitted to the extent the data protection laws and the Collective Bargaining Agreement N° 68 are complied with; the employer must clearly define the purposes of such monitoring, and if it is only to monitor the employees, the use of the CCTV must be temporary.

14.2 Is consent or notice required? Describe how employers typically obtain consent or provide notice.

Consent is not required as it would not be freely given, taking into account the imbalance of power between the employer and the employee. Fair processing notices are always required. Employers usually inform the workers of the monitoring via the Work Regulations, via a specific policy or, when it is punctual, before the monitoring activity.

14.3 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?

Pursuant to Collective Bargaining Agreement N° 68 on the protection of privacy of workers with regard to CCTV in the workplace and Collective Bargaining Agreement N° 81 concerning the protection of workers’ private lives in respect of the monitoring of electronic communications in the workplace, the Works Council or, in the absence of a Works Council, the Committee for Health and Safety or the employee representatives, must be informed of the use of CCTV in the workplace and the monitoring of electronic communications in the workplace.

15 Data Security and Data Breach

15.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?

Yes, personal data must be processed in a way which ensures security and safeguards against unauthorised or unlawful processing, accidental loss, destruction and damage of the data.

Both controllers and processors must ensure they have appropriate technical and organisational measures to meet the requirements of the GDPR. Depending on the security risk, this may include the encryption of personal data, the ability to ensure the ongoing confidentiality, integrity and resilience of processing systems, an ability to restore access to data following a technical or physical incident, and a process for regularly testing and evaluating the technical and organisational measures for ensuring the security of processing.

15.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

The controller is responsible for reporting a personal data breach without undue delay (and in any case within 72 hours of first becoming aware of the breach) to the Data Protection Authority, unless the breach is unlikely to result in a risk to the rights and freedoms of the data subject(s). A processor must notify any data breach to the controller without undue delay.

The notification must include the nature of the personal data breach including the categories and number of data subjects concerned, the name and contact details of the Data Protection Officer or relevant point of contact, the likely consequences of the breach and the
measures taken to address the breach, including attempts to mitigate possible adverse effects.

15.3 **Is there a legal requirement to report data breaches to affected data subjects?** If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

Controllers have a legal requirement to communicate the breach to the data subject, without undue delay, if the breach is likely to result in a high risk to the rights and freedoms of the data subject.

The notification must include the name and contact details of the Data Protection Officer (or point of contact), the likely consequences of the breach and any measures taken to remedy or mitigate the breach.

The controller may be exempt from notifying the data subject if the risk of harm is remote (e.g., because the affected data is encrypted), the controller has taken measures to minimise the risk of harm (e.g., suspending affected accounts) or the notification requires a disproportionate effort (e.g., a public notice of the breach).

15.4 **What are the maximum penalties for data security breaches?**

The maximum penalty is the higher of EUR 20,000,000 or 4% of worldwide turnover.

### 16 Enforcement and Sanctions

#### 16.1 Describe the enforcement powers of the data protection authority(ies).

<table>
<thead>
<tr>
<th>Investigatory Powers</th>
<th>Civil/Administrative Sanction</th>
<th>Criminal Sanction</th>
</tr>
</thead>
<tbody>
<tr>
<td>Investigative Powers</td>
<td>The Data Protection Authority has wide powers to order the controller and the processor to provide any information it requires for the performance of its tasks, to conduct investigations in the form of data protection audits, to carry out reviews on certificates issued pursuant to the GDPR, to notify the controller or processor of alleged infringement of the GDPR, to access all personal data and all information necessary for the performance of controllers’ or processors’ tasks and access to the premises of the data including any data processing equipment.</td>
<td>N/A</td>
</tr>
<tr>
<td>Corrective Powers</td>
<td>The Data Protection Authority has a wide range of powers, including to issue warnings or reprimands for non-compliance, to order the controller to disclose a personal data breach to the data subject, to impose a permanent or temporary ban on processing, to withdraw a certification and to impose an administrative fine (as below).</td>
<td>N/A</td>
</tr>
</tbody>
</table>

#### 16.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?

The GDPR entitles the relevant data protection authority to impose a temporary or definitive limitation, including a ban on processing. Pursuant to the Law of 3 December 2017 on the establishment of the Data Protection Authority, the inspection chamber of the Data Protection Authority can order by way of temporary measure the suspension, limitation or freezing of the processing under review, if the data concerned could cause damage which is serious, immediate and difficult to repair. The dispute chamber can order the temporary or definitive freezing, restriction or prohibition of the processing.

#### 16.3 Describe the data protection authority’s approach to exercising those powers, with examples of recent cases.

It is too soon to know the Data Protection Authority’s approach to exercising its powers under the GDPR. Before the Law of 3 December 2017 on the establishment of the Data Protection Authority, the Commission for the Protection of Privacy did not have the power to issue a ban on a particular processing activity. However, it could institute proceedings against the controller before the regular courts and tribunals in order to obtain such a ban or transfer the matter to the Public Prosecutor for criminal proceedings against the controller. In 2017, the Commission for the Protection of Privacy instituted proceedings against Facebook before the Court of First Instance in Brussels. On 16 February 2018, the Brussels Court of First Instance condemned Facebook for having tracked internet users without their knowledge or consent, and ordered the ceasing of the unlawful processing under penalty of a fine of EUR 250,000 per day with a maximum of EUR 100,000,000.

#### 16.4 Does the data protection authority ever exercise its powers against businesses established in other jurisdictions? If so, how is this enforced?

The Data Protection Authority does indeed exercise its powers against businesses established in other jurisdictions. On 16 February 2018, the Brussels Court of First Instance condemned Facebook, including Facebook Ireland Limited and Facebook Inc., for having
tracked internet users without their knowledge or consent. The court ordered the ceasing of the unlawful processing under the penalty of a fine of EUR 250,000 per day with a maximum of EUR 100,000,000. The judgment has, however, been appealed by Facebook and the matter will now be heard by the Court of Appeals.

17 E-discovery / Disclosure to Foreign Law Enforcement Agencies

17.1 How do businesses typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?

Where e-discovery requests or requests for disclosure from foreign law enforcement agencies require a transfer of personal data to non-EEA countries not offering adequate protection of personal data, businesses typically either (i) agree on appropriate safeguards with the recipient (if and to the extent possible), (ii) seek the explicit consent of the data subjects for the disclosure and transfer, (iii) limit the disclosure to anonymous data, and/or (iv) provide a legal opinion from a reputable law firm to confirm that the disclosure and transfer is not permitted under applicable data protection laws.

17.2 What guidance has/have the data protection authority(ies) issued?

The WP29 has issued an Opinion 1/2009 on pre-trial discovery for cross-border litigation, which provides guidance to controllers subject to EU law in dealing with requests to transfer personal data to another jurisdiction for use in civil litigation. The Data Protection Authority has not issued any specific opinions on the subject, but has indicated (amongst others, in an opinion of 2008 on the SWIFT case) that it follows the opinion of the WP29.

18 Trends and Developments

18.1 What enforcement trends have emerged during the previous 12 months? Describe any relevant case law.

The Data Protection Authority is determined to act against large international businesses that do not comply with the applicable data protection legislation. This is illustrated, amongst others, by the investigations that the Data Protection Authority has carried out into the activities of Facebook. In 2015, the Commission for the Protection of Privacy issued a recommendation and a letter of default to Facebook for violations of the restrictions on cookies. As a result of that, Facebook was convicted for the first time in 2015, after which the Court of Appeals ruled in favour of Facebook on 16 June 2016. However, the Commission for the Protection of Privacy started new proceedings against Facebook in 2017 and obtained a favourable decision from the Brussels Court of First Instance on 16 February 2018. The judgment has, however, been appealed by Facebook and the matter will now be heard by the Court of Appeals.

18.2 What “hot topics” are currently a focus for the data protection regulator?

The Data Protection Authority has recently been focusing on the following “hot topics”:

- restructuring of the internal organisation of the Data Protection Authority: since 25 May 2018, the Belgian Data Protection Authority has lacked a five-member Executive Committee. This is likely to be resolved in 2019, as the Executive Committee is expected to be appointed in March 2019.
- GDPR compliance: the Data Protection Authority has put a lot of effort into raising awareness with and educating (i) businesses, large and small, on their obligations under the GDPR, and (ii) citizens on their (new) rights under the GDPR in connection with the processing of personal data;
- the privacy of minors: the Data Protection Authority has been raising awareness among young people concerning the protection of their privacy online;
- image rights: the Data Protection Authority has developed the theme of image rights, both towards young people and their parents; and
- the fight against terrorism and violent radicalism: the Data Protection Authority has issued several opinions on this issue.
Bastiaan Bruyndonckx
Lydian
Avenue du Port 86C b113
1000 Brussels
Belgium
Tel: +32 2 787 90 93
Email: bastiaan.bruyndonckx@lydian.be
URL: www.lydian.be

Bastiaan is a Partner in Lydian’s Commercial & Litigation department and heads the Information & Communications Technology (ICT) practice as well as the Information Governance & Data Protection (Privacy) practice.

Bastiaan has a particular focus on information governance, privacy, data protection and cybersecurity and advises businesses in a broad range of industry sectors.

Bastiaan is a fellow of the Belgian American Educational Foundation (BAEF) and is a member of the International Association of Privacy Professionals (IAPP).

Bastiaan is a regular speaker at seminars, workshops and conferences on privacy and data protection. He also regularly publishes in international legal reviews such as Computerrecht, Privacy & Informatie, DataGuidance and Bulletin des Assurances. Bastiaan also contributed to the book Data Protection – The Impact of the GDPR in Insurance with a chapter regarding the new rules on consent and the processing of special categories of data under the GDPR.

Olivia Santantonio
Lydian
Avenue du Port 86C b113
1000 Brussels
Belgium
Tel: +32 2 787 90 07
Email: olivia.santantonio@lydian.be
URL: www.lydian.be

Olivia is a Senior Associate in Lydian’s Information Governance & Data Protection (Privacy) practice and IP and ICT practice.

Olivia frequently advises on data protection issues regarding, inter alia, the obligations and liability of the data controller and data processor, the transfer of data into and out of the EU and the processing of sensitive data. She often drafts and reviews privacy policies as well as data processing agreements. She also specialises in global privacy issues (GDPR compliance, contracts review, binding corporate rules, etc.).

Olivia is regularly invited as a speaker at conferences and seminars, including on the GDPR.

Olivia is a member of the International Association of Privacy Professionals (IAPP) and an active member of the International Association for the Protection of Intellectual Property (AIPPI).

Our Information Governance & Data Protection (Privacy) team represents clients, large and small, from all industry sectors (including technology, retail, telecommunications, health care and life sciences, media, energy, insurance, banks and other financial institutions, as well as printing and publishing industries) on all aspects of information governance and data protection.

Our range of services includes corporate privacy risk management, (GDPR) compliance, international data transfers, records management, e-discovery, (direct) marketing, e-commerce, cybersecurity and cybercrime.

We provide assistance to our clients, from legal advice to integrated consulting on corporate privacy risk management, as well as legislative strategic policy advice and legal compliance. We also litigate on behalf of clients in data protection-related matters.

We advise clients on global data protection and privacy compliance challenges, including by taking into account data protection and privacy rules on a global basis. We frequently advise clients on multi-jurisdictional data protection (privacy) compliance projects, either dealing with the local Belgian aspects or leading the project for our client with the support of local correspondent firms advising on local law issues.

Lydian is one of the few independent law firms in Belgium operating outside a US/UK law firm banner. We are a popular referral choice for foreign firms seeking a high-quality law firm in Belgium with recognised skills in data protection, such as Berwin Leighton Paisner, Burgess Salmon, Hogan Lovells, Luther, Norton Rose Fulbright, Taylor Wessing and Willkie Farr & Gallagher.
Chapter 9

Brazil

Vaz E Dias Advogados & Associados

José Carlos Vaz E Dias

1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

On August 14, 2018, Federal Law 13,709 (the so-called “Lei Geral de Proteção de Dados” or “General Data Protection Law” or “LGPD”), was enacted in Brazil, which protects private data and provides for the processing of personal data, including on digital platforms, and deals with “sensitive personal data”. It further modified Law 12,965 of April 23, 2014 (known as the “Internet Law”). The Internet Law deals specifically with business and consumer transactions and matters of a private nature transmitted on digital platforms through the internet.

The LGPD was amended by Provisional Measure (“MP”) 869 of December 27, 2018. This Law created the National Authority for the Protection of Data (“ANPD”). Further to that, it extended the vacatio legis of the LGPD for 24 months as from August 14, 2018. This means that the LGPD will be in force and fully applicable as from August 14, 2020.

It is important to state that the LGPD does not apply to or regulate business-to-business (“B2B”) information, or to other kinds of personal data processing, such as that which is:

(a) Produced by a natural person for exclusively private and non-economic purposes.
(b) Produced exclusively for journalistic, artistic and academic purposes.
(c) Produced for the following reasons: public security, national defence, safety of the country and criminal investigation and penalties. Such processing will be ruled by specific law.
(d) Originating not in the Brazilian territory and which is not subject to communication, shared use of data with Brazilian processing agents or international transfer of data with other country than the country of origin insofar as the country of origin provides a degree of personal data protection compatible with the terms and conditions set by the LGPD.

1.2 Is there any other general legislation that impacts data protection?

There is further legislation in Brazil that impacts on the level of personal data protection, as it deals with specific sectors and transactions, as follows:

1) Federal Law 12,965 of April 23, 2014 (known as the “Internet Law”) and its regulation (Decree 8,771 of May 11, 2016) are relevant to data protection. The Internet Law establishes the principles, rights and obligations regarding the use of the internet in Brazil. It deals with the relationship between the provider and the internet user. Moreover, this law addresses the collection, storage, use and grant to third parties of access to private data through the internet (connection logs to which this law relates). It ensures that the contents of private communications and transfers to third parties comply with the protection of privacy, private life, honour and the image of the involved parties.

The Internet Law is recognised as of utmost importance to data protection in view of the increasing use of information stored and transmitted electronically and business transactions made online. According to a research published in 2017, Brazil had nearly 140 million internet users in 2016. Additionally, monthly internet usage in Brazil amounted to 25.7 hours per user in 2017 and 90% of Brazilian internet users accessed the internet every day for personal reasons (https://www.statista.com/topics/2045/internet-usage-in-brazil/). Therefore, the internet is a powerful tool used in Brazil for producing and transferring personal data, especially in commerce.

2) The Consumer Rights Code – Federal Law 8,078 of September 11, 1990 – addresses the collection and use of consumers’ data exploited for business purposes. Paragraph 2 of Article 43, for example, expressly determines that the creation of files and databases, and the registration of personal data and data related to commerce, should first be communicated to consumers. Consumers will have full access to the registered and gathered information about them and be able to request the rectification of incorrect collected data. This rule derives directly from Item X of Article 5 of the Federal Constitution.

By means of Decree 7,962 of March 15, 2013, new specific rules were set for those consumers that buy products or hire services through the internet. Such rules deal essentially with three aspects of consumer rights: (i) clear information about the products and services provided by the supplier through the internet; (ii) transparent rules for consumers; and (iii) right to regret and to cancel the transaction.

Further to that, Federal Law 13,543 of December 19, 2017 sets the obligation for internet providers to disclose ostensive and clear information to consumers when offering services/products through the internet. In this regard, the law establishes that such disclosure should be in text that is clearly visible to the consumer, and in a font size no smaller than 12.

The third relevant piece of legislation is Federal Law 10,406 of January 10, 2002 (the so-called “Brazilian Civil Code” or “Law of the Common Man”). It revised concepts established by the Civil Code of 1916, adopted new principles and took into consideration new human and business relationships. This law established for the first time a specific section –
Chapter II of Title I of Book I – comprising 11 articles ruling about privacy, private life, honour and the image of a person (so-called personality rights). There is a clear objective to protect the moral integrity of a person against possible third-party interference or unauthorised use of third parties. Therefore, legal measures may be granted to prevent violation of private life. The Brazilian Civil Code further recognises that personal events can only be exposed followed by the consent of the individual owning the rights and in some other specific situations, such as court orders.

(4) The fourth general piece of legislation is the Criminal Code (Decree-Law 2,848 of December 7, 1940), which provides in its Articles 150–154 offences for disclosing information regarding residence, private location, private correspondence and messages and information regarded as of a confidential nature. A new offence was added to the Criminal Code in 2012 (by Law 12,737 of November 30, 2012) related to the private life of individuals. Accordingly, it is an offence for a person to invade or hack computers or devices with the purpose of obtaining, collecting, displaying or destroying data or information without the authorisation of the holder. The penalty is up to two years of imprisonment.

1.3 Is there any sector-specific legislation that impacts data protection?

There is further legislation that affects data for specific sectors or activities and that forms the legal framework for data protection in Brazil. This is as follows:

- **Item XXXIII of Article 5 and Item II of Paragraph 3 of Article 37 of the Federal Constitution (Habeas Data)**

  These grant to all persons the right to receive from public agencies information of private interest regarding such person or of collective or general interest stored in any public agency, except information whose secrecy is essential to the national security of society.

- **Federal Law 12,527 of November 18, 2011 (Freedom of Information Act)**

  This establishes procedures for all persons and citizens to request to public agencies the contents of private information and data and to update and rectify any incorrect information available in public databases.

- **Complementary Law 105 of January 10, 2001 (Financial Transaction Confidentiality)**

  This addresses confidentiality related to transactions and storage of private information performed by financial institution operating in Brazil. The general rules include the obligation of financial institutions to maintain safe and secret any collected information of their active and passive transactions and services rendered. Further, it sets out that the disclosure of private information of a person may only be done when expressly consented to by the person. It also establishes the exceptions to these rules when special events take place, such as illicit activities, smuggling, terrorism, money laundering and corruption, among others. It establishes fines and penalties for the breach of confidentiality.

- **Federal Law 9,279 of May 15, 1996 (Industrial Property Rights Law)**

  The Industrial Property Rights Law stipulates in its Article 195 specific events regarded as a violation of confidentiality information in trade. Item XIV of Article 195 for example deals with the exploitation or use of clinical test data. Accordingly, the unauthorised exploitation and use of clinical tests or other undisclosed data whose preparation involves considerable effort and that were submitted to public agencies for obtaining approval for a product’s commercialisation is a crime. This rule specifically addresses data exclusivity of clinical trials. Besides the fact that data exclusivity is an investment in the pharma industry, it is recognised that the collected data in clinical trials comprises personal information about people that participate in the trials and is thereby regarded as personal data. Nevertheless, Item XIV of Article 195 lacks further legal developments.

1.4 What authority(ies) are responsible for data protection?

The “General Data Protection Law” by means of MP 869 of December 27, 2018 established the ANPD, which is a government entity under the federal public administration and duly empowered to address the following matters:

(a) Guarantee the protection of personal data.

(b) Establish regulations and procedures on the protection of personal data.

(c) Hold discussions at the administrative level on the interpretation of the LGPD and applicable laws, the ANPD’s authorities and matters on which the LGPD is silent.

(d) Request information from controllers and operators of personal data that deals with personal data processing operations.

(e) Adopt simplified procedures, including those by electronic platforms for the registration of complaints about personal data treatment that does not comply with the LGPD.

(f) Monitor and apply sanctions for data processing that does not conform with the legislation by means of administrative procedures that guarantee rights to adversary proceedings, broad defence and appeal.

(g) Inform the competent authorities about criminal offences of which it has knowledge.

(h) Inform the internal control bodies of any violations of the LGPD committed by bodies and entities of the federal public government.

(i) Disclose to the population information about the rules and public policies for the protection of personal data and security measures.

(j) Stimulate the adoption of standards for services and products that ease the exercise of control and protection of titleholders on their personal data, taking into account the peculiarities of the activities and the size of the responsible parties.

(k) Perform studies on local and international practices related to the protection of personal data and privacy.

(l) Promote cooperation with authorities involved in the protection of personal data of other countries, of international or transnational nature.

(m) Lead public consultations to gather suggestions about relevant matters of public interest in the scope of the ANPD’s activities.

(n) Carry out, prior to the publications of resolutions, adequate hearings on public administration entities or bodies responsible for the regulation of specific sectors of the economy.

(o) Coordinate with public regulatory authorities to exert their authority in specific sectors of economic and government activities that are required to be regulated.

(p) Issue annual administration reports about its activities.

According to MP 468/2019, the ANPD’s powers will prevail over the authority of other entities of the public administration related to personal data protection. Further to that, the ANPD will preserve business confidentiality and secrecy of information, under the terms of the law.
2 Definitions

2.1 Please provide the key definitions used in the relevant legislation:

- **“Personal Data”**
  It is understood as a piece of compiled information or data related to an identified or identifiable natural person, including identifying numbers, location data or electronic identification when these are related to a person as well as that found in private communication whether or not it is exchanged on the internet.

- **“Processing”**
  This expression means any operation carried out with personal data, including collection, production, reception, classification, use, access, reproduction, transmission, distribution, processing, archiving, storage, elimination, evaluation or control of information, communication, modification, transfer, dissemination or extraction.

- **“Controller”**
  The term “controller” means the natural or legal person, private or public, that is competent to take decisions related to the treatment of personal data.

- **“Processor”**
  The term “processor” means a natural or legal person of public or private nature that processes personal data in the name and on behalf of a controller.

- **“Data Subject”**
  It is understood as the physical person to which the private information relates to and which is subject to processing.

- **“Sensitive Personal Data”**
  This term means, under the LGPD, personal data of a physical person related to racial or ethnic origin, religious beliefs, political opinion, affiliation to unions or other religious organisations, philosophical or political nature, data related to the health or sexual life of a person, genetic information or biometric data.

- **“Data Breach”**
  Data breach encompasses the following infringement events, among others:
  (1) The use, exploitation and disclosure of private/personal information without the express, free and informed consent of the person identified by it or in accordance with the cases provided by law.
  (2) The transfer or access to third parties of private information, whether or not for commercial purposes, without the prior, express and clear consent of the person identified by it or in accordance with cases provided by law.
  (3) The denial of access to private information to the person identified by it for revision, update, elimination and rectification purposes.
  (4) The supply of unclear and/or incomplete information about the policy on the collection, use, storage, processing and protection of users’ personal data and connected records and records of access to internet applications.
  (5) Retention and the making available to third parties of connections logs and access to internet applications logs as well personal data and the content of private communication without the adequate respect for privacy, private life and honour.

- **“Anonymised Data”**
  It is a piece of personal information that at the time of proceeding loses the possibility of direct and indirect association to a natural person.

- **“Consenting”**
  This term means the free authorisation, informed and unequivocal communication by means of which the data subjects agrees with the processing of its personal data for a specific purpose.

- **“Classified Information”**
  “Classified information” is a piece of information which is temporarily unavailable to the public due to its relevance to social and state security (this concept is provided by the Freedom of Information Act).

- **“Pseudonymisation”**
  Processing of private data by means of which data loses the ability to associate directly or indirectly with the natural person, except for the use of additional information maintained separately by the controller in a safe environment.

3 Territorial Scope

3.1 Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to those laws?

Data protection applies to any natural or legal person, public or private, irrespective of the means, of the country and the headquarters in which the natural or legal company/controller is located, or of the country in which the data are located, insofar as the following requirements are fulfilled:

1. the processing activities are realised in the Brazilian territory;
2. the processing activities aim to offer or supply goods and services in the Brazilian territory or relate to private data of individuals that were in Brazil when the data were collected; and
3. the personal data subject to processing have been collected in the Brazilian territory. Personal data collected in the Brazilian territory are looked upon as those data whose data subject is in the Brazilian territory at the time of the collection.

This means that the LGPD will apply regardless of the nationality of the data subject, the place of the headquarters of controller and the manner in which the data will be processed.

The Internet Law further sets out in Paragraph 1 of Article 11 that any operation of collection, storage, retention and treatment of personal data or communication data by connection providers extends to entities located overseas, if at least one of such processing activities takes place in the Brazilian territory. Further to that, the Internet Law applies to foreign companies that collect data in Brazil and to the content of communications in relation to which at least one of the terminals is placed in Brazil or in case they offer services in Brazil or at least one member of the same economic group (internet service provider) is established in Brazil.

4 Key Principles

4.1 What are the key principles that apply to the processing of personal data?

- **Transparency**
  The transparency of collected and stored information is an LGPD Principle derived from Item X of Article 5 of the Federal Constitution. This Item protects private information and gives full access to the collected and stored data for possible update, modification and deletion by the involved person.
According to the LGPD, this Principle is expressed as the guarantee to data subjects that precise, clear, important and accessible information will be provided to them and processing agents processing such data are subject to business secrecy.

- **Lawful basis for processing**

  The lawful basis for processing is a Principle that shapes the LGPD and other specific laws on data protection, especially Decree 8,771/2016 (regulating the Internet Law). This Principle sets out the importance for controllers to adopt transparency vis-à-vis data subjects as to processing information. It further recommends providers to adopt guidelines setting security standards for personal data and private communication, including processing, storage and disposal, for individuals whose personal data is concerned.

  Based on the Principle of Lawful Basis for Processing, Article 7 of the LGPD establishes the events under which personal data can be processed by the controller, as follows:

  - When the data subject provides his/her consent to processing.
  - When the controller needs to fulfil a legal or regulatory obligation.
  - When the processing is needed for the execution of public policies prescribed in laws and regulations or when grounded on agreements, partnership or similar instruments, subject to the provisions of Chapter IV of the LGPD.
  - When required for the realisation of studies by research institutions, securing whenever possible the anonymisation of the personal data.
  - When required for the execution of an agreement or preliminary proceedings related to an agreement in which the data subject is a part of it, at the request of the data subject.
  - When required for the regular exercise of rights in court actions, administrative proceedings or arbitration, following the terms of Law 9,307 of September 21, 1996 (the so-called Arbitration Law).
  - When required for the protection of life or the physical safety of the data subject or of third parties.
  - When required for the protection of health in procedures led by professionals of the health field or by sanitation entities.
  - When required to attend the legitimate interest of a controller or of third parties, except when regarding the fundamental rights and liberties of the data subject that demand the protection of personal data. Legitimate interest takes place when controllers process personal data for legitimate purposes in the following events: (a) support and promotion of controllers’ activities; and (b) protection of the regular exercise of their rights or provisions of services that benefit them, always taking into account the legitimate expectations and the fundamental rights and liberties set out by the LGPD.
  - When required for the protection of credit, as provided in the specific and applicable legislation.

Consent is not needed when the personal data of a data subject is essentially of public knowledge.

- **Purpose limitation**

  The Purpose Limitation Principle prevails in the existing data protection framework as the concept that the upload, collection and use of information about a person, including that related to communication data, should be limited and directly related to the purpose for which it was retained, stored and used.

  The LGPD highlights this principle by clearly establishing in Item 1 of Articles 6, 7 and 10 that the processing activities of personal data shall need to be specific and legitimate, and only the personal data strictly required for the desired purpose may be processed. Therefore, the law does not permit processing which is incompatible with the set limitation.

  On this matter, Article 12 of Decree 8,771/2016 (the Internet Law) clearly sets out that “connection and applications providers must retain as little personal data, private communications and connection and access to application records as possible”. In addition, it determines that the retained and stored information should be deleted after the purpose of its use is achieved and the set legal deadline for data storage (as stipulated in the Internet Law) is complied with. Collection, use, storage, processing and protection of users’ personal data may take place when such acts are adequately justified, are not prohibited by the laws of the land and are specifically provided in the terms and conditions of the internet service agreement.

- **Data minimisation**

  The LGPD recognises the Data Minimisation Principle and therefore sets out that the collection and storage of personal data should be kept to a minimum and be specifically related to the purpose of their processing.

- **Proportionality**

  The right to collect, store, retrieve and upload personal data and data linked to internet connection records and records of access to internet applications, among others, needs to conform to the purpose set out by the LGPD, to the legitimate interest of the controller, and to the limits set by the Brazilian Constitution. Therefore, the processing may be viewed under the balance of rights – between the intimacy and private rights of the data subject and the rights of the controller.

- **Accuracy**

  Under the Accuracy Principle, data subjects may update and eliminate personal data any time the processed information is inaccurate and contains an error.

  Further, the Consumers Right Law also establishes the need of consumers to receive accurate and true information about an individual when companies and entities collect or provide information about a consumer or operate a consumer database. Consumers also include companies or legal entities receiving products or services from a supplier. This is defined in the Consumer Rights Code as any individual or legal entity that obtains or uses products or services as an end-user. Therefore, private information at the consumer level also involves that of legal entities.

- **Retention**

  The Retention Principle is also known under the LGPD as the Security Principle. It derives from the Internet Law, as this Principle was already in this piece of law. Accordingly, it stipulates that the internet provider or holder of the internet connection or of personal data information must maintain the connection records (private information) under confidentiality and in a controlled and safe environment for a period of one year in accordance with the regulation. The responsibility for the maintenance of the data and connection records during this period cannot be transferred to third parties. As for application access logs, the internet provider needs to maintain these under confidentiality and in a controlled and safe environment for six months.

  Under the LGPD, the Principle of Retention is provided under the obligation of the controller to use all technical and administrative measures to protect the personal data from unauthorised access and accidental or unlawful destruction, loss, alteration, communication or diffusion.

  The Consumer Rights Code further stipulates in Paragraph 1 of Article 43 the prohibition to maintain negative data about consumers in a database for a period longer than five years, independently of the fact that the consumer might still be in debt to the business.
Other key principles – please specify

There are additional key principles provided by the LGPD and the Brazilian Internet Law that secure specific protection for a data subject of its personal data and the limits of such, as follows:

1) **Non-discrimination Principle** – This Principle guides existing rules and measures set by the LGPD that prevent processing for illicit, abusive and discriminatory purposes.

2) **Liability Principle and Account** – This Principle requires the controller and the agent to evidence the adoption of effective measures to confirm that the controller is fulfilling the applicable rules for the protection of personal data.

3) **Publicity Principle** – This Principle guides agencies of the public administration holding personal data of individuals. Its main purpose is guarantee of access by individuals and companies/entities to any private information held by public entities and agencies. According to this Principle, the right to make data available is looked upon as a rule and the only exception regards secrecy.

4) **Disclosure of Information of a Public Interest Principle** – This Principle is set out by the Freedom of Information Act and aims to secure access to information, especially that in the public interest, irrespective of requests from the owner or the identified individual.

5) **Free Speech Principle** – This is secured to individuals against possible fake and wrong information kept in a database or publicised to third parties, including the right to oppose any information provided by the controller.

### 5 Individual Rights

#### 5.1 What are the key rights that individuals have in relation to the processing of their personal data?

- **Right of access to data/copies of data**
  
  The right of any individual to access private information is secured in Brazil by case law based on the right of privacy and private life provided by Item X of Clause 5 of the Brazilian Constitution.

  The LGPD further supports individuals’ rights by securing adequate ownership of the personal data to data subjects and the right of intimacy and privacy under the concept of the law. Following this individual right, data subjects are entitled to obtain from controllers the access to their private information, including: whether or not personal data is being processed by the controller; correction of inaccurate information or incomplete or outdated data; and anonymisation. Data subjects may eliminate or block excessive and unnecessary data held by the controller or which is considered to be in violation of the LGPD; obtain portability of the data to another service or product provider by means of express request; and ensure that portability will respect the concepts of confidentiality and eliminate processed personal data with the data subject’s consent, except in the case of termination of data processing, as provided by Article 16 of the LGPD.

  Also, Article 43 of the Consumer Rights Code grants to consumers the access to companies’ files and databases specifically created to compile information about them, their lives and habits. The Internet Law further secures to any individual full access to the private information collected and stored by internet providers and others.

- **Right to rectification of errors**
  
  The right to rectify errors and update information is guaranteed for an individual or data subject when the information is processed by a controller. The LGPD provides further broad individual rights that comprise the right to freedom and privacy. Under the right to freedom, the LGPD secures to data subjects the right to request a controller to correct wrong and inaccurate data, and complete and update its personal data. To strengthen such right to rectify errors, data subjects may further petition before the supervisory authority (ANPD) and demand the rectification or alteration of data.

  The Consumer Rights Code provides further for the rectification of errors, as stipulated by Paragraph 3 of Article 43. Such provision allows consumers to immediately correct and eliminate imprecise and incorrect information in a file or record or database, including information provided by internet providers. When requested by a consumer, database holders will have five (5) weekdays to communicate the change of this incorrect/imprecise information to any parties involved, including the data subjects.

- **Right to deletion/right to be forgotten**
  
  The right to delete existing personal data and be forgotten is regarded as a fundamental right secured to data subjects insofar as the following requirements are fulfilled: (i) the personal data needs to be processed by controller; (ii) the personal data is no longer needed for the proposed objective of collection and processing; (iii) the personal data is excessively collected and processed; (iv) the personal data does not comply with the provisions of the law; and (v) the data subject expressly communicates revocation of their consent and the controller has no overriding grounds to justify the processing.

The exceptions to this rule are provided by the LGPD for situations where conservation of data is of importance to studies by a research body (securing whenever possible the anonymisation of personal data), where the controller is required to keep the data in order to comply with any legal or regulatory obligation and where the transfer of data to third parties is required by law.

The Internet Law further secures to internet users in Item X of Article 7 the ability for definitive elimination of any personal data given for the use of a certain internet application at the end of the relationship between the internet user (individual) and the internet provider. Such right to delete does not prevail over mandatory log retention, as specified by the applicable laws and court orders.

- **Right to object to processing**
  
  Processing may be opposed by data subjects when the processing does not comply with the requirements of the LGPD and when processing is based on the peculiar situation of data subjects that demands specific and stringent measures for the approval of processing. For example, sensitive personal data may only be processed in some specific situations, such as for the regular exercise of rights and for the protection of life and health. The same rationale applies to personal data of children and adolescents. Therefore, in some specific situations, controllers need to cease the processing of personal data when data subjects oppose processing, unless the controller evidences legitimate rights for the processing that overrides the fundamental rights secured to data subjects.

Further to the LGPD, the Internet Law provides in Item IX of Article 7 that the express consent of the individual for the collection, use, storage and processing of personal data is required. This consent needs to be addressed and obtained through a specific separate contractual clause. Further, it is an obligation of internet providers to supply clear and complete information on the collection, use, storage, processing and protection of users’ personal data.

The same rights are found in the Consumer Rights Code, including express consent.

There are discussions about the validity period of the express consent and therefore whether express consent may be...
terminated at any time by the individual, which will permit objections to the processing of information. The discussion lies on the fact that intimacy and private life are regarded by Article 11 of the Civil Code as personality rights. Therefore, they cannot be transmitted or renounced, and they cannot be voluntarily limited. On the other hand, both the Internet Law and the Consumer Rights Code value the transparency principle, which provides that once the individual adheres to the “User Agreement and Privacy Policy”, he/she needs to comply with its terms and conditions. The common understanding is that individuals adhering to a specific “User Agreement and Privacy Policy” should comply with its terms and conditions, but provisions restricting the prior consent for the processing, transfer of information to third parties and others rights secured by the law cannot be eliminated or disposed of by the involved parties (the individual and the provider). Therefore, such violations would grant the user the right to object to processing.

- **Right to restrict processing**

Data subjects also have the right to restrict the processing of their personal data under the rulings and guidance of LGPD. Accordingly, restriction may be requested by data subjects to make the processing comply with the legitimate purposes of the controller and exclude data that does not support and promote the activities of controller. Further to that, restrictions may take place when the processing period has lapsed and in other situations where justification for processing no longer exists, but the conservation and use by controller are still required for specific purposes, such as to comply with legal and regulatory obligations. Restriction is further guaranteed to data subjects for sensitive data and data related to children and adolescents where compliance with strict rules is required.

Both the Consumer Rights Code and the Internet Law also secure to individuals the right to restrict processing, including non-disclosure to third parties, of personal data, connection records and records of access to internet applications. The exception to this right would take place in case individuals expressly and freely consent to the transfer of files to third parties or in accordance with the cases provided by law, such as court orders and access by the administrative authorities to recorded data regarding personal qualification, affiliation and address.

- **Right to data portability**

Data subjects have the right to request and access the personal data in a specific format that favours the right to access the data, including machine-readable format. The information and data will be provided at the discretion of the data subjects by electronic means, in a printed form or by means of a complete statement indicating the origin of the data, the inexistence of registration, the criteria used, the purpose of the processing and the possible transfer of rights from one controller to another.

- **Right to withdraw consent**

The consent of data subjects to controllers for processing their personal data may be revoked at any time the data subjects decide upon, as long as there is no request to stop processing the personal data. The elimination of the personal data shall take place after termination of the processing of data. The right to withdraw consent should be a free and facilitated procedure and it does not interfere with the validity and effectiveness of the processing carried out with the previous consent.

- **Right to object to marketing**

Data subjects hold the right to hamper the processing of personal data with the objective of marketing. Sensitive personal data and data of children and adolescents suffer restrictions as to marketing by the controller, unless the marketing of the information is relevant to protect life and health under the terms of Article 11 of the LGPD.

- **Right to complain to the relevant data protection authority(ies)**

The right to complain to the supervisory authority against unlawful processing and other activities of the controller is secured to data subjects, as provided by Paragraph 1 of Article 18 of the LGPD. Upon complaint to the supervisory authority, the processing of personal data will be terminated due to breach of the provisions of the LGPD.

Other key rights – please specify

- **Right to basic information**

The right to obtain basic information about a controller, the purposes of processing personal data and other information related to processing is regarded as a fundamental right of data subjects. According to Article 9 of the LGPD, data subjects are entitled to have facilitated access to the information on the processing of their data and therefore the controller should ensure the transfer of transparent, direct and clear information about the processing to data subjects.

### 6 Registration Formalities and Prior Approval

#### 6.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?

No. There are no registration requirements for processing private data by a businessman, as the use and processing of private data by a controller is regarded as a private matter, although the LGPD is a law of public order.

#### 6.2 If such registration/notification is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?

This is not applicable to Brazil.

#### 6.3 On what basis are registrations/notifications made (e.g., per legal entity, per processing purpose, per data category, per system or database)?

This is not applicable to Brazil.

#### 6.4 Who must register with/notify the data protection authority (e.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation)?

This is not applicable to Brazil.

#### 6.5 What information must be included in the registration/notification (e.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes)?

This is not applicable to Brazil.
6.6 What are the sanctions for failure to register/notify where required?

This is not applicable to Brazil.

6.7 What is the fee per registration/notice (if applicable)?

This is not applicable to Brazil.

6.8 How frequently must registrations/notifications be renewed (if applicable)?

This is not applicable to Brazil.

6.9 Is any prior approval required from the data protection regulator?

This is not applicable to Brazil.

6.10 Can the registration/notification be completed online?

This is not applicable to Brazil.

6.11 Is there a publicly available list of completed registrations/notifications?

This is not applicable to Brazil.

6.12 How long does a typical registration/notification process take?

This is not applicable to Brazil.

7 Appointment of a Data Protection Officer

7.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.

Following the terms of the LGPD, the appointment of a Data Protection Officer is mandatory, as this person will act as a communication channel between the controller, the data subjects and the ANPD. In view of the mandatory appointment, complaints have been made about the cost impact of such appointment on local and foreign companies that offer goods and services in Brazil. Nevertheless, it is understood that Data Protection Officers should have a technical and legal background, including extensive knowledge on the internet and compliance, and have specific competences that vary according to the need of the controller and data subjects.

7.2 What are the sanctions for failing to appoint a Data Protection Officer where required?

Failing to appoint a Data Protection Officer does not create any specific sanctions against the controller. Therefore, non-compliance with this requirement will apply the general sanctions available under the LGPD, including fines and blockage of personal data.

7.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect of his or her role as a Data Protection Officer?

Data Protection Officers are not protected from disciplinary measures or employment obligations. Whether or not the Data Protection Officer is an employee of the controller, his/her action is regarded as independent and specifically related to the LGPD. Therefore, non-compliance with the Data Protection Officer’s duties (not as an employee) will make the Data Protection Officer responsible for such acts and consequences.

Although the LGPD does not extensively address the powers, limits and consequences of the Data Protection Officer. It is understood that its activity is framed as a mandate under Article 653 of the Brazilian Civil Code. Under this article, the party empowered to undertake a specific task on behalf of others is responsible for its mandated acts.

7.4 Can a business appoint a single Data Protection Officer to cover multiple entities?

The LGPD does not provide expressly any restrictions on the appointment of a single Data Protection Officer to represent different entities or controllers. Therefore, a group of companies could appoint a single Data Protection Officer to undertake the specified tasks under the LGPD insofar as the identity and contact information about the Data Protection Office is clear, made public and objectively disclosed to data subjects.

7.5 Please describe any specific qualifications for the Data Protection Officer required by law.

The LGPD does not provide any professional, academic and personal qualification requirements for Data Protection Officers. Therefore, any person can be empowered by a controller to exercise the activities of channelling communications between the controller, the data subjects and the supervisory authority.

Nevertheless, it is understood that Data Protection Officers should have a technical and legal background, including extensive knowledge on the internet and compliance, and have specific competences that vary according to the need of the controller and data subjects.

7.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?

The responsibilities of the Data Protection Officer are:

1) receiving and accepting complaints and communications from data subjects as well as supplying clarifications and taking adequate measures to solve the identified problems;
2) receiving communications from the ANPD and taking appropriate measures;
3) instructing employees and contractors of the entity on the good practices to be adopted in relation to personal data protection;
4) carrying out any other duties established by the controller or in supplementary rules; and
5) cooperating with the ANPD.

7.7 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?

The LGPD does not provide any requirement for registration and/or notification of the Data Protection Officer with the ANPD or other authorities, especially for validation purposes.

7.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?

Yes. The Data Protection Officer needs to be named and hold contact data disclosed in a public-facing privacy notice, such as on the controller’s website or in an equivalent document. Such disclosure should comprise clear and objective information about the Data Protection Officer.

8 Appointment of Processors

8.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?

No. The LGPD does not demand any kind of agreement for the indication and appointment of a processor by a controller. Such indication may be done orally or in the form of a written agreement and may comprise specific responsibilities beyond those provided by the LGPD, such as keeping a record of the personal data processing operations carried out by processors and controllers. Processor shall carry out the processing in accordance with instructions supplied by controller, which shall set compliance, instructions and the rules on the matter.

8.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?

Although the LGPD does not demand the use of an agreement to bind a controller and processor, the adoption of such agreement is of importance so that the rights, obligations and responsibilities of the processor are adequately and clearly established. One should remember that a processor needs to strictly follow controllers’ directions. Further to that, a processor is jointly liable for any losses and damages caused by the processing of personal data when the processor fails to comply with the obligations of the data protection law or fails to follow the lawful instructions of controller.

In view of the activities to be carried out by the processor, it is recommended that the agreement between controller and processor takes place by a written and specific agreement.

9 Marketing

9.1 Please describe any legislative restrictions on the sending of electronic direct marketing (e.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?).

The National Telecommunication Agency (“ANATEL”) has issued specific regulations determining corrective measures for sending marketing materials through SMS and emails. According to Circular Letter 39/2012/PVCP/PVCP – ANATEL – marketing may be sent, but it is required for mobile users to receive an SMS message allowing the user to express its interest in no longer receiving marketing messages (contract opt-in format). If the user does not want to receive further messages, the user will have the right to send a free SMS stating the word LEAVE. The user will necessarily receive a message stating “Message received with success. From now on you will not receive additional marketing messages from this service provider”.

Further to that, ANATEL has determined a 12-word format for agreements between the mobile telecommunication provider and the user (consumer) in order to facilitate reading by the consumer as well as other requirements, as follows:

- The SMS may only be sent during commercial hours.
- The SMS may not be sent on Sundays and holidays.
- Maximum of 140 to 160 characters.
- The sender needs to identify itself in the final message.
- Dissemination of ideas of political and religious nature are prohibited.
- Identification of the subject matter must be linked to the marketing message.
- The consumer has the option to leave and no longer receive messages from the sender or the company (opt-out message).

In case consumers do not receive the opt-out message, they may cancel the marketing messages by sending the word “LEAVE” to a specific number of the mobile company.

Regarding advertising regulations, direct contact for marketing purposes to a consumer at home or work may be classified as illegal and abusive, under Item IV of Article 6 of the Consumer Rights Code, when undertaken by means of dishonest and coercive business methods and without the consumer’s prior approval.

9.2 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.).

The Consumer Rights Code provides a ruling for the offer of products and services, including through telephone and postal reimbursement. For marketing or sale by phone or postal reimbursement, the offer needs to specify the name of the manufacturer and address on the package, any publicity and in all printed material used in the commercial transaction. Further, advertising of goods and services by telephone is prohibited when the call is onerous to the consumer who receives it.

9.3 Do the restrictions noted above apply to marketing sent from other jurisdictions?

Yes, such restrictions apply to marketing sent from other countries as they violate consumers’ rights. Accordingly, consumers may
9.4 Is/are the relevant data protection authority(ies) active in enforcement of breach of marketing restrictions?

Breaches of marketing restrictions are enforced by consumers and there is no specific authority that can enforce breaches of marketing restrictions.

9.5 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?

The purchase of marketing lists from third parties is not prohibited under the applicable laws insofar as the individual, company or entity under which the private data is traded have been originally informed about the seller that their personal data could be transferred to third parties or when the transfer of the files and information to a third party is expressly authorised. Further, a third party needs to implement adequate security measures, as provided by the LGPD and by Articles 7, 8, 11, 12, 13, 14, 15, 16 and 17 of the Internet Law.

The Consumer Rights Code further frames abusive and unfair commercial practices, including those not in accordance with the Code, as offences.

9.6 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?

Sending marketing communications in breach of the Brazilian Internet Law may be subject to losses and damages and the following penalties:

- A warning.
- Fines of up to 10% of the revenue of the company or internet provider in Brazil.
- Suspension or prohibition of data collection and storage activities.

According to Article 56 of the Consumer Rights Code, administrative sanctions applied by specific agencies created by the federal, state and local governments may include the following, among others:

- Fines and product seizure.
- Prohibition of production and commercialisation of the illegally advertised product.
- Temporary suspension of the company’s activities.
- Revocation of the licence to exercise commercial activities.

10 Cookies

10.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).

The LGPD does not specifically address the use of cookies or other similar technologies and therefore cookies are permitted. Since cookies are instruments to collect private information, it is understood that their use should comply with the following requirements:

- Prior and/or express consent of the person is adequately given; and
- Storage and keeping of connection records, and the security and confidentiality measures are informed to the individual, as provided by the LGPD, the Internet Law and the Consumer Rights Code.

10.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?

There is no law with provisions regarding cookies and therefore the general rules on intimacy rights, personal data (the LGPD) and consumer rights apply. Where cookies do not identify the individual but gather general information about individuals and consumers without distinguishing them, prior consent and the rules provided do not apply.

10.3 To date, has/have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?

This question does not apply, since there is no data protection authority applicable for the regulation of cookies unless the cookies are framed as processed private data under the LGPD.

10.4 What are the maximum penalties for breaches of applicable cookie restrictions?

The answers provided in question 9.6 above apply to the breach of applicable cookie restrictions as well as those provided by the LGPD.

11 Restrictions on International Data Transfers

11.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.

According to the LGPD, international transfer of data is the transfer of personal data to a foreign country or international organisation of which the country is a member. Prior consent is needed for such consent, unless:

1) The transfer is to countries or international organisations that provide the appropriate level of protection of personal data provided by the LGPD.

2) The controller provides and evidences guarantees of compliance with the principles, rights of the data subject and data protection regime established in the LGPD, in the form of:

- a) specific contractual sections for a given transfer;
- b) standard contractual sections;
c) in case of international corporate rules; and
d) seals, certificates and codes of conduct regularly issued.

3) The transfer is required for international legal cooperation between government intelligence, investigation and police bodies, in accordance with international legal instruments.

4) The transfer is required for the protection of life or physical integrity of the data subject or any third party.

5) The ANPD authorises such transfer.

6) The transfer results in a commitment undertaken under an international cooperation agreement.

7) The transfer is required for enforcement of a public policy or legal attribution of the public utility, upon disclosure of the provisions of item I of the main provision of Article 23 of the LGPD.

8) The data subject has provided specific and highlighted consent for such transfer, with previous information on the international nature of the operation, clearly distinguishing it from any other purposes.

9) Where required to address the situations specified in items II, V and VI of article 7 of the LGPD, such as for compliance with a statutory or regulatory obligation by the controller or the regular exercise of rights in court, administrative or arbitration procedures.

11.2 Please describe the mechanisms businesses typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).

To our knowledge, the following procedures must be complied with in the transfer of local personal data to other countries:

- Execution of a transfer agreement.
- Compliance with the foreign exchange control laws and taxation applicable in case payment for the transfer of private data to foreign parties takes place.
- Provision of guidelines or detailed information to the individual about the storage and use of their data, including access logs to connections and internet applications records.
- Provision of the transfer agreement rules set by the Internet Law, as these are indispensable for the transfer of files and access to information by third parties.
- Provision of adequate and clear information to the individual about the foreign rules that will be applicable to the transfer of their personal data that may affect the validity and enforceability of their data protection rights.

As a result, the transfer of personal data to other countries will require compliance with the transparency and prior and written consent rules and the provision of adequate information to the individual to which the personal data refers.

The aforementioned procedures for international transfer of personal data do not comply necessarily with the rules of the LGPD, since this piece of legislation was enacted on August 14, 2018 and it is not in force at the moment.

11.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.

There is no such registration or notification or prior approval by the ANPD for the international transfer of data. However, the level of data protection of the foreign country or international organisation shall be assessed by the ANPD, which will take into account the nature of the data, the general and sectorial rules of the applicable law in the country of destination or international organisation, the compliance with the general principles of protection to personal data, the adoption of security measures provided for by the regulations and any other specific circumstances related to the transfer of information.

12 Whistle-blower Hotlines

12.1 What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?

Federal Law 13,608 of January 11, 2018 authorised the set-up of hotlines to receive reports and rewards for information that supports police investigations in the prevention and repression of crimes or administrative offences.

This Federal Law further sets out the obligations of transport companies that operate under concessions by the federal, state and municipal government to exhibit in their vehicles a “Dial Complaint” sign, thereby permitting complaints of any kind that may assist police investigations about existing facts.

One of the most important rulings of this law is the guarantee that informants will have their name and private data kept fully confidential, therefore complying with the inviolability of privacy and private life assured by the Federal Constitution.

Although Brazil does not have specific ruling and laws, besides Federal Law 13,608/2018, dealing with whistle-blower hotlines, it is recognised that companies and public and private entities may adopt such programmes. However, private data of informants and those reported in the investigation should be kept confidential until the criminal offence is confirmed and made public by the authorities.

12.2 Is anonymous reporting prohibited, strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do businesses typically address this issue?

Anonymous reporting is generally permitted, taking into account that information or the provided report aims to assist an investigation into the veracity of facts. Corporate anonymous reports should be published with great care so that private information, especially that not related to the report and names of people, are not unduly made public.

13 CCTV

13.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?

There is no regulation in Brazil dealing with CCTV systems that record people in public or private areas. Therefore, there is no data protection authority or rules dealing with specific forms of public notice.
13.2 Are there limits on the purposes for which CCTV data may be used?

CCTV recording requires compliance with the inviolability of intimacy and private life principles and the need to use such CCTV strictly for its intended purpose in a specific place. If CCTV data is collected for monitoring possible trespassing, it cannot be used for other purposes.

14 Employee Monitoring

14.1 What types of employee monitoring are permitted (if any), and in what circumstances?

Employee monitoring or surveillance is not regulated under Brazilian law. It is shaped instead by case law and scholars’ reasoning. Such practices are allowed insofar as the employee’s privacy rights (also encompassed by Item X of Article 5 of the Federal Constitution) are not violated and the adopted surveillance measures are justified and applied proportionally for achieving the proposed objectives. Therefore, monitoring employees to protect the company’s property and competitive information regarding trade secrets is fully acceptable. It is recommended however that monitoring procedures and measures be adequately and clearly informed to the employees, including access to the companies’ computers and emails.

Labour courts understand that personal devices (bags, purses, etc.) are covered by an employee’s right to privacy. Therefore, a company must obtain free and informed consent from the employee to monitor and access personal devices and/or letting them know that monitoring and searches may occur in specific situations.

14.2 Is consent or notice required? Describe how employers typically obtain consent or provide notice.

Access to devices owned by the company in use by its employees does not require prior consent, but employees should be always informed that the work devices are of a professional nature and not private. Therefore, it is recommended for a company to tailor specific guidelines to ensure that employees clearly know the boundaries between private information and the company’s information and access to such.

14.3 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?

No work council, trade representatives or trade unions need to be notified or consulted to adopt surveillance measures, as the monitoring of employees is not regulated by law.

15 Data Security and Data Breach

15.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?

The LGPD sets standards for security and confidentiality of personal data and private communications. The standards aim to prevent that the processing leads to the violation of data by unauthorised accesses and accidental or unlawful situations of destruction, loss, modification, communication or any form of inappropriate or unlawful processing. This involves the ANPD being granted the ability to set minimum technical standards which are required to be implemented by controllers and processors.

Therefore, controllers and processors, within the scope of their authority for personal data processing, individually or by means of associations, may elaborate good practices and governance ruling that provide for organisation conditions, operation system, procedures, including complaints and petitions of data subjects, security rules, technical standards, specific obligations for the different parties involved in the processing, educative actions, internal mechanisms of supervision and risk mitigation, and any other aspects relating to personal data processing.

On this matter, the controller, with due regard for the structure, level and volume of its operations, and the sensitivity of the treated data and the likelihood and severity of damages to data subjects, may undertake the following measures:

1) Adopt a privacy governance programme that shall at least:
   a) evidence the controller’s commitment to adopt internal processes and policies that ensure broad compliance with rules and good practices concerning personal data protection;
   b) be applicable to the entire set of personal data under its control, regardless of the manner in which it carried out the collection thereof;
   c) be adapted to the structure, level and volume of its operations, and to the sensitivity of the treated data;
   d) establish appropriate policies and safeguards based on a process of systematic assessment of impacts on and risks to the privacy;
   e) be intended to establish a trust relationship with the data subject, by means of transparent actions that ensure mechanisms of participation of the data subject;
   f) be integrated to its general governance structure and establish and apply internal and external supervision mechanisms;
   g) have an incident response and remediation plan; and
   h) be constantly updated based on information obtained from continuous monitoring and periodic assessments.

2) Demonstrate the effectiveness of its privacy governance programme when appropriate, especially at the request of the supervisory authority or any other entity in charge of promoting compliance with good practices or codes of conduct, which independently promote compliance with this law.

15.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

Yes. In case of a breach of personal data, the controller shall notify the ANPD and the data subject of the occurrence of any security incident that may result in any relevant risk or damage to the data subjects. Such notice shall be delivered within a reasonable term, as defined by the supervisory authority, and contain at least: (a) the description of the nature of the affected personal data; (b) the information on the data subjects involved; (c) the indication of the technical and security measures used for data protection, with due regard for trade and industrial secrets; (d) the risks relating to the incident; (e) the reasons for the delay, if in case the notice is not
16.1 Describe the enforcement powers of the data protection authority(ies).

<table>
<thead>
<tr>
<th>Investigatory Power</th>
<th>Civil/Administrative Sanction</th>
<th>Criminal Sanction</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advisory and Authorization Nature</td>
<td>ANPD holds extensive power to supervise, advise and authorise the processing of personal data. ANPD shall establish rules for progressive adequacy of databases created by the date of effectiveness of this law, taking into account the complexity of the processing operations and the data's nature.</td>
<td>No power to apply criminal sanctions.</td>
</tr>
<tr>
<td>Investigative Nature</td>
<td>The penalties shall be imposed after an administrative proceeding that provides the chance for a broad defence, on a gradual, individual or cumulative basis, in accordance with the peculiarities of the relevant case and parameters set out by the LGPD.</td>
<td>No power to apply criminal sanctions.</td>
</tr>
</tbody>
</table>

16.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?

Yes. The ANPD holds the power to issue a ban on a peculiar processing activity with the involvement of a court order. The penalties shall be imposed after an administrative proceeding that provides the chance for a broad defence, on a gradual, individual or cumulative basis, in accordance with the peculiarities of the relevant case and parameters set out by the LGPD.

16.3 Describe the data protection authority’s approach to exercising those powers, with examples of recent cases.

There are no recent cases, as the law has not been in force due to the vacatio legis stipulated by the LGPD.

16.4 Does the data protection authority ever exercise its powers against businesses established in other jurisdictions? If so, how is this enforced?

As yet, there have been no instances of this in practice in Brazil.

17 E-discovery / Disclosure to Foreign Law Enforcement Agencies

17.1 How do businesses typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?

Brazilian companies are required to respond to e-discovery requests by providing adequate information on electronic data that may be used as evidence of criminal or civil charges. Adequate information means answering the questions in the e-discovery requests and providing full access to any private data specified in the e-discovery. Nevertheless, the delivery of information and data needs to be supported by a court order. On this matter, we highlight that the use, disclosure and transfer of private data to any third parties needs to be expressly authorised by the individual to which the private information relates or, as an exception, by a court order in case of possible infringement of data protection.

Further, e-discovery requests must comply with the procedures of the Brazilian Civil Procedural Code, which requires confirmation of the country in which the plaintiff requesting the e-discovery is
18. Trends and Developments

18.1 What enforcement trends have emerged during the previous 12 months? Describe any relevant case law.

Most notable is the effective creation of the ANPD, deriving from MP 869 of December 27, 2018, such kind of legislation being of a temporary nature. Whether the ANPD will be an autonomous entity with no subordination to other agencies and entities is yet to be resolved.

18.2 What “hot topics” are currently a focus for the data protection regulator?

The biggest issue for data protection regulators and/or judges is the legal treatment of “fake news” in view of the general elections for the presidency and the Federal Members of Parliament, which took place in October/November 2018.

Recently, the Federal government and the local press have been complaining about the amount of fake news on the death of a member of Rio de Janeiro’s parliament – Mrs. Marielle – who was assassinated by “hired people” on March 14, 2018. Most of the fake news has been attempting to relate her death to drug trafficking or paramilitary groups. It is believed, however, that her assassination occurred due to her activities in favour of the poor and black people and against police abuse.

Although the Internet Law has provided adequately for several issues related to data protection, fake news and its sometimes-devastating effects are issues which concern the authorities and legislators. Judicial authorities have called on Congress to pass comprehensive rules dealing with fake news and penalties for publishing such that affect the electoral process, public safety and public health.

A court decision that possibly highlights the unfair competition practice of fake news was issued in November 7, 2016 by the 11th Civil Chamber of the State Court of São Paulo involving the subsidiary of the Chinese company Baidu Brasil Internet Ltda. against the defendant PSAFE TECNOLOGIA S.A. The case – Civil Action TJP n°. 1006564-47.2015.8.26.0100 – involved the request by PSAFE TECNOLOGIA S.A. to interrupt the sale of the application (“app”) “Du Speed Booster” of Baidu, for the equipment that operates via the Android system, through the virtual store “Google Play”, until Baidu made the necessary changes in order not to send fake information about “PSafe Total”. PSAFE TECNOLOGIA S.A. wanted “PSafe Total” to no longer be identified as a virus.

The problem derived from Baidu’s practice of making public, through its website and social media, false information on “PSafe Total”. Baidu claimed that this app was infected with a virus and that it was malware. Further to that, Baidu programmed its app “Du Speed Booster” to send false alerts to users stating that “PSafe Total” was malware and recommending the user to uninstall “PSafe Total”. Therefore, Baidu’s practice was regarded as unfair competition against “PSafe Total”, a Brazilian startup focused on digital security. Baidu was ordered to pay losses and damages for this unfair practice, to be determined in due process, and a fine that may reach 20% of Baidu’s gross revenue.

Further to that, Baidu will be obliged to issue public messages on its websites and social media channels, informing the public about the propagation of untrue information on “PSafe Total”. It was further required to modify its app “Du Speed Booster” so that it no longer sends false alerts on “PSafe Total”.

The law firm Vaz E Dias Advogados & Associados is specialised in intellectual property law and focuses on assisting foreign and local companies in the protection of intangibles and providing legal support for business transactions that explore intellectual knowledge and technological innovation. The firm’s legal activities also involve legal support for the protection and exploitation of image and personality rights, especially of actors, sportsmen and those who suffer exploitation of their image rights by the media. The firm is also involved in the implementation of confidentiality and data protection policies for the guarantee of secret information and access to private information, commercial pledge of intellectual property rights, assignment of trademarks and patents, technology transfer and licensing agreements, franchising, image rights usage, copyright and entertainment law. The firm’s legal activities encompass aspects related to the protection of technological inventions through patents and utility models, to the registration of industrial design, plant varieties, semiconductors, trademarks, domain names, copyright and their efficacy in the Brazilian territory.

José Carlos Vaz E Dias Advogados & Associados
Rua da Assembleia 10
Conjunto 2422 – Centro
Rio De Janeiro
Brazil
Tel: +55 21 3176 6530
Email: jose.dias@vdav.com.br
URL: www.vdav.com.br

José Carlos Vaz E Dias is an attorney-at-law, has been specialised in intellectual property law since 1990 and is a partner of the intellectual property law firm Vaz E Dias Advogados & Associados. His expertise includes the enforcement of patents, know-how and repression of unfair competition activities. He has special knowledge on licensing agreements of intellectual property, personality rights, data protection, sports law and entertainment law, regarding which he provides legal support to artists and sport professionals.

José Carlos Vaz E Dias holds an LL.M. and Ph.D. from the University of Kent in Canterbury (England). He is also a Professor of the State University of Rio de Janeiro (UERJ) where he teaches intellectual property rights law.
Canada

Osler, Hoskin & Harcourt LLP

1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

Private Sector Privacy Laws in Canada

There are four private sector privacy statutes that govern the collection, use, disclosure and management of personal information in Canada: (i) the Federal Personal Information Protection and Electronic Documents Act, S.C. 2000, ch. 5 (“PIPEDA”); (ii) Alberta’s Personal Information Protection Act, S.A. 2003, ch. P-6.5 (“PIPA Alberta”); (iii) British Columbia’s Personal Information Protection Act, S.B.C. 2003, ch. 63 (“PIPA BC”); and (iv) Québec’s An Act Respecting the Protection of Personal Information in the Private Sector, R.S.Q., ch. P-39.1 (“Québec Privacy Act”). Collectively, these will be referred to hereinafter as “Canadian Privacy Statutes” and will be the main focus of this chapter.

The Federal private sector law, PIPEDA, governs the inter-provincial and international collection, use and disclosure of personal information. It applies to personal information (including employee information) held by federally regulated businesses, such as banks, airlines, railways, telecommunications companies and internet service providers, across the country.

PIPEDA also applies generally to personal information (excluding employee information) that is collected, used and disclosed by organisations in the course of a commercial activity which takes place within a province that does not otherwise have “substantially similar” legislation.

The private sector privacy statutes in Alberta, British Columbia and Québec (referenced above) have each been deemed “substantially similar” to PIPEDA and, as such, PIPEDA will not apply to commercial organisations operating within those jurisdictions, other than federally-regulated businesses which continue to be covered by PIPEDA regardless.

The health privacy statutes in Ontario, New Brunswick, Newfoundland & Labrador and Nova Scotia have also been deemed substantially similar to PIPEDA, and therefore, PIPEDA does not apply in respect of private health providers operating within those jurisdictions but continues to apply to other commercial activity therein. (See the response to question 1.3 for information on health privacy legislation in Canada.)

Public Sector Privacy Laws in Canada

Federal, provincial and territorial laws otherwise govern all public sector institutions within each of their respective jurisdictions.

1.2 Is there any other general legislation that impacts data protection?

Canada has enacted anti-spam legislation entitled An Act to Promote the Efficiency and Adaptability of the Canadian Economy by Regulating Certain Activities that Discourage Reliance on Electronic Means of Carrying Out Commercial Activities, and to Amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act, S.C. 2010, c. 23 (“Canada’s anti-spam legislation” or “CASL”). (See the response to question 9.1 for details.)

British Columbia (Privacy Act, R.S.B.C. 1996, c. 373), Saskatchewan (Privacy Act, R.S.S. 1978 c. Chapter P-24), Manitoba (Privacy Act, C.C.S.M., c. P125) and Newfoundland and Labrador (Privacy Act, RSNL1990, c. P-22) have also each adopted a statutory tort of invasion of privacy.

Québec civil law also provides individuals with a right to privacy under the Civil Code of Québec, CQLR, c. CQ-1991 and the Québec Charter of Human Rights and Freedoms, CQLR, c. C-12.

1.3 Is there any sector-specific legislation that impacts data protection?

Yes. Most of the provinces in Canada have enacted health privacy legislation that applies to health information custodians in the context of providing healthcare services.

1.4 What authority(ies) are responsible for data protection?

Each Canadian jurisdiction – federally, provincially and territorially – has its own independent Information and Privacy Commissioner who reports to their respective legislature and oversees the relevant data protection laws applicable in that jurisdiction.

2 Definitions

2.1 Please provide the key definitions used in the relevant legislation:

- “Personal Data”
  “Personal Data” (“Personal Information”) is defined very broadly under Canadian Privacy Statutes as information...
about an identifiable individual. Generally, information will be deemed to be about an “identifiable individual” where it is reasonably possible for an individual to be identified through the use of that information, alone or in combination with other available information.

- **“Processing”**
  “Processing” is not expressly defined under Canadian Privacy Statutes but, in practice, would include the collection, use, modification, storage, disclosure or destruction of personal information.

- **“Controller”**
  “Controller” is not expressly defined under Canadian Privacy Statutes. Canadian Privacy Statutes refer to “organizations” more generally, which include controllers.

- **“Processor”**
  “Processor” is not defined under Canadian Privacy Statutes. Canadian Privacy Statutes refer to “organizations” more generally, which include processors.

- **“Data Subject”**
  “Data Subject” is not defined under Canadian Privacy Statutes. Canadian Privacy Statutes refer to individuals.

- **“Sensitive Personal Data”**
  “Sensitive Personal Data” is not defined under Canadian Privacy Statutes. PIPEDA provides that “any information can be sensitive depending on the context”.

- **“Data Breach”**
  PIPEDA defines a “breach of security safeguards” as “the loss of, unauthorized access to or unauthorized disclosure of personal information resulting from a breach of an organization’s safeguards that are referred to in clause 4.7 of Schedule 1 or from a failure to establish those safeguards”.

  PIPA AB does not define “Data Breach” but requires notification to the Alberta Information and Privacy Commissioner who may, in turn, require notification to affected individuals “of any incident involving the loss of, or unauthorized access to, or disclosure of, the personal information where a reasonable person would consider that there exists a real risk of significant harm to an individual as a result of the loss or unauthorized access or disclosure”.

- **Other key definitions**
  There are no other key definitions in particular.

### 3 Territorial Scope

#### 3.1 Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to those laws?

Although PIPEDA is silent with respect to its territorial reach, the Federal Court of Canada has found that PIPEDA will apply to businesses established in other jurisdictions if there is a “real and substantial connection” between the organisation’s activities and Canada. With respect to websites, relevant connecting factors include: (1) where promotional efforts are being targeted; (2) the location of end-users; (3) the source of the content on the website; (4) the location of the website operator; and (5) the location of the host server.

### 4 Key Principles

#### 4.1 What are the key principles that apply to the processing of personal data?

- **Transparency**
  Under the Transparency principle (also referred to as “Openness”), Canadian Privacy Statutes require organisations to document and make readily available to individuals, in a form that is generally understandable, specific information about their policies and practices relating to the management of personal information.

- **Lawful basis for processing**
  In general, Canadian Privacy Statutes require organisations to obtain consent for the collection, use and disclosure of personal information, subject to limited exceptions. In order for consent to be valid, it must be reasonable to expect that individuals would understand the nature, purpose and consequences of the collection, use or disclosure of the personal information to which they are consenting. An organisation shall not require consent as a condition for providing a product or service, beyond that required to fulfil an explicitly specified and legitimate purpose. The form of consent (express or implied) may vary depending on the nature of the information and the reasonable expectations of the individual. Individuals may withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice.

  Canadian Privacy Statutes contain a general obligation that personal information must be collected by fair and lawful means (i.e., consent must not be obtained through deception, coercion or misleading practices).

  Even with valid consent, organisations are subject to an overarching legal requirement that personal information can only be collected, used and disclosed for purposes that a reasonable person would consider appropriate in the circumstances. See the Proportionality principle below.

- **Purpose limitation**
  Organisations are generally required to identify the purposes for which personal information is collected at or before the time the information is collected. Organisations shall also document such purposes in accordance with the Transparency principle; see above.

  Personal information must not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. See also the Data minimisation and Proportionality principles.

- **Data minimisation**
  Canadian Privacy Statutes generally require that the collection, use and disclosure of personal information be limited (both in type and volume) to the extent to which it is necessary to fulfil the purposes identified by the organisation. Personal information shall not be retained longer than necessary to fulfil those purposes. See the Retention principle below.

- **Proportionality**
  Canadian Privacy Statutes generally set out the overriding obligation that organisations may only collect, use and disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances.

  The principle of Proportionality is also built into some of the other principles. For example, the safeguarding obligation imposed on organisations is proportional to the level of sensitivity, whereby the more sensitive the information, the higher the level of protection will be required. See the Safeguarding principle below. Similarly, the extent to which personal information shall be accurate, complete and up to
date will depend upon the use being made of the information, taking into account the interests of the individual. See the Accuracy principle below.

■ Retention

In keeping with the Data Minimisation principle above, Canadian Privacy Statutes generally require organisations to retain personal information for only as long as necessary to fulfill the purposes for which it was collected, subject to a valid legal requirement.

Personal information that is no longer required to fulfill the identified purposes should be destroyed, erased or made anonymous.

Organisations should develop guidelines and implement procedures for retention of personal data, including minimum and maximum retention periods and procedures governing the destruction of data.

■ Other key principles – please specify

Accountability – Canadian Privacy Statutes reflect the key principle of accountability. Organisations are responsible for protecting personal information under their control, including personal information that they transfer to third parties for processing, for which they must ensure a comparable level of protection through contractual or other means.

Organisations must designate and identify an individual who is accountable for the organisation’s compliance with the other privacy principles and shall implement policies and practices to give effect to those principles.

Safeguarding – Each of the Canadian Privacy Statutes contains specific provisions relating to the safeguarding of personal information. In essence, these provisions require organisations to implement reasonable technical, physical and administrative measures to protect personal information against loss or theft, as well as unauthorised access, disclosure, copying, use, modification or destruction.

Accuracy – Canadian Privacy Statutes contain obligations for organisations to ensure that personal information in their records is accurate, complete and up to date, particularly where the information is used to make a decision about the individual to whom the information relates or is likely to be disclosed to another organisation.

5 Individual Rights

5.1 What are the key rights that individuals have in relation to the processing of their personal data?

■ Right of access to data/copies of data

Under Canadian Privacy Statutes, organisations must, upon request and subject to limited exemptions, inform individuals of the existence, use and disclosure of his or her personal information, and must give them access to that information, including a listing of the third-party organisations with whom the information has been shared.

The right of “access” does not oblige an organisation to provide copies of personal information records; rather, it requires the provision of access, which may include viewing the records at the organisation’s offices. Generally, an individual’s request must be sufficiently specific as to allow an organisation to identify responsive records. The organisation must respond within a prescribed time limit, or a reasonable period, as the case may be, at minimal or no cost to the individual, and must make the information available in a form that is generally understandable.

The exemptions to the right of access vary among the statutes and need to be carefully considered. Examples of the statutory exemptions include, but are not limited to, information subject to solicitor-client or litigation privilege, confidential commercial information, information about another individual, information that relates to national security matters and information generated in a formal dispute resolution process.

■ Right to rectification of errors

Canadian Privacy Statutes generally require that when an individual demonstrates the inaccuracy or incompleteness of his or her personal information held by an organisation, the organisation must correct the inaccuracies and/or add a notation to the information, as appropriate.

■ Right to deletion/right to be forgotten

While Canadian Privacy Statutes afford individuals the right to withdraw consent and challenge the accuracy, completeness and currency of their personal data, they do not grant a specific right to require organisations to “erase” or delete their personal information per se.

■ Right to object to processing

Although Canadian Privacy Statutes do not include a specific right to object to processing, they prohibit organisations from requiring, as a condition for providing a product or service, that individuals give consent to the collection, use or disclosure of their personal information beyond that which is required to fulfill the explicitly specified and legitimate purpose. Also, an individual must be able to withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice. Upon receipt of any withdrawal, individuals must be informed of the implications of such withdrawal.

■ Right to restrict processing

See above.

■ Right to data portability

Although Canadian Privacy Statutes include a right of access to personal information (see above), they do not include a right to data portability.

■ Right to withdraw consent

Under Canadian Privacy Statutes, an individual must be able to withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice. Individuals must be informed of the implications of such withdrawal.

■ Right to object to marketing

Consent is required for the collection, use or disclosure of personal information for marketing purposes. The form of consent required (opt-in or opt-out) will vary depending on the circumstances, the sensitivity of the information and the reasonable expectations of the individual. In cases where opt-out consent is appropriate, individuals must be made aware of the marketing purposes at or before the time of collection, and in a manner that is clear and understandable. Individuals must be able to easily opt out of the practice; the opt-out must take effect immediately and be persistent; and the information collected and used must be destroyed or effectively de-identified as soon as possible thereafter. (See also the response to question 9.1.)

■ Right to complain to the relevant data protection authority(ies)

Under Canadian Privacy Statutes, individuals have a right to make a complaint to the relevant data protection authority. Prior to this, individuals must be able to address data protection issues with the designated individual within the organisation who is accountable for the organisation’s compliance. (See the Accountability principle above.) Organisations must have easy-to-access and simple-to-use procedures in place to respond to complaints or inquiries and must take steps to effectively address complaints accordingly.
### 6 Registration Formalities and Prior Approval

**6.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?**

Generally, businesses do not have any legal obligation to register with or notify the relevant data protection regulatory authorities in respect of processing activities. Exceptionally, organisations that wish to use or disclose personal information without consent for statistical or scholarly study or research purposes must (in addition to other conditions) notify the Federal Privacy Commissioner before such use or disclosure.

*(See the response to question 15.2 for notification requirements in the event of data breaches.)*

**6.2 If such registration/notice is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?**

This is not applicable.

**6.3 On what basis are registrations/notifications made (e.g., per legal entity, per processing purpose, per data category, per system or database)?**

This is not applicable.

**6.4 Who must register with/notify the data protection authority (e.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation)?**

This is not applicable.

**6.5 What information must be included in the registration/notification (e.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes)?**

This is not applicable.

**6.6 What are the sanctions for failure to register/notify where required?**

This is not applicable.

**6.7 What is the fee per registration/notification (if applicable)?**

This is not applicable.

**6.8 How frequently must registrations/notifications be renewed (if applicable)?**

This is not applicable.

**6.9 Is any prior approval required from the data protection regulator?**

This is not applicable.

**6.10 Can the registration/notification be completed online?**

This is not applicable.

**6.11 Is there a publicly available list of completed registrations/notifications?**

This is not applicable.

**6.12 How long does a typical registration/notification process take?**

This is not applicable.

### 7 Appointment of a Data Protection Officer

**7.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.**

PIPEDA, PIPA Alberta and PIPA BC expressly require organisations to appoint an individual who is accountable for ensuring compliance with the organisation’s data protection obligations and who may, in turn, delegate some of his or her responsibilities to others. Such individuals are typically referred to as the Chief Privacy Officer or Privacy Officer, though Canadian Privacy Statutes do not prescribe any particular title.

**7.2 What are the sanctions for failing to appoint a Data Protection Officer where required?**

There are no specific sanctions for failure to appoint a Privacy Officer.

**7.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect to his or her role as a Data Protection Officer?**

Canadian Privacy Statutes do not protect Privacy Officers against disciplinary measures as a specific function of their role. However, Privacy Officers, like other employees, enjoy some protection against retaliatory action of their employer when they, acting in good faith and based on reasonable belief, refuse to do something that will contravene the relevant data protection statute, or conversely, do something in an attempt to bring them into compliance therewith.
7.4 Can a business appoint a single Data Protection Officer to cover multiple entities?

There is no specific statutory provision that either allows or prohibits this.

7.5 Please describe any specific qualifications for the Data Protection Officer required by law.

Canadian Privacy Statutes do not set out any specific qualifications for the Privacy Officer. In a guidance document entitled *Getting Accountability Right with a Privacy Management Program* (hereinafter, “*Getting Accountability Right*”), the Federal, British Columbia and Alberta privacy regulators set out what the role of the Privacy Officer should entail, and their expectation that he or she be supported by proper training, resources and staff. Practically, a Privacy Officer would be expected to have a broad-based skill set, particularly with respect to compliance and risk management, as well as familiarity with the legal and regulatory frameworks under Canadian Privacy Statutes.

7.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?

At law, a Privacy Officer is generally responsible for ensuring the organisation’s compliance with the applicable privacy statute.

In *Getting Accountability Right*, the Federal, British Columbia and Alberta privacy regulatory authorities describe the role of the Privacy Officer more specifically as the individual who is accountable for structuring, designing and managing the programme, including all procedures, training, monitoring/auditing, documentation, evaluation, and follow-up. Depending on the type and size of the organisation, these Canadian privacy regulatory authorities expect the Privacy Officer to, among other things: establish and implement programme controls, in coordination with other appropriate persons responsible for related functions within the organisation; be responsible for the ongoing assessment and revision of programme controls; represent the organisation in the event of a complaint investigation by a Privacy Commissioner’s office; and most critically, advocate privacy protection within the organisation itself.

7.7 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?

There is no requirement to register or notify the Data Protection Officer with the relevant data protection authorities.

7.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?

Organisations must be open about, and make available in a form that is generally understandable, the contact information of the person who is accountable for the organisation’s policies and practices and to whom complaints or inquiries can be made. Canadian privacy regulatory authorities expect the Privacy Officer’s contact information to be included in a public-facing privacy policy.

8 Appointment of Processors

8.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?

Yes, under PIPEDA, an organisation is required to “use contractual or other means to provide a comparable level of protection while the information is being processed by a third party.” The failure to have appropriate confidentiality agreements in place with third-party contractors has been found to be a breach of the accountability principle.

8.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?

In the private sector context, Canadian Privacy Statutes do not specify the requirements to be included in agreements with third-party processors. However, some privacy laws, and their accompanying regulations, in the health sector for instance, more expressly set out the terms and conditions to be included in written agreements between institutions and information managers. (*See, for example, section 66 of Alberta’s Health Information Act, R.S.A. 2000, c. H-5, and accompanying Regulation 70/2001.*)

9 Marketing

9.1 Please describe any legislative restrictions on the sending of electronic direct marketing (e.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?).

The sending of email and SMS text messages is subject to both the requirements under Canadian Privacy Statutes and Canada’s anti-spam legislation (“CASL”). In general, under CASL, it is a violation to send, or cause or permit to be sent, a commercial electronic message (defined broadly to include text, sound, voice or image messages) to an electronic address unless the recipient has provided express or implied consent (as defined in the Act) and the message complies with the prescribed form and content requirements, including an “unsubscribe” mechanism.

9.2 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.).

Telephone marketing in Canada is subject to the requirements of Canadian Privacy Statutes as well as the Canadian Radio-Television and Telecommunications Commission’s (“CRTC”) Unsolicited Telecommunications Rules. These rules include specific requirements related to the National Do-Not-Call List (“National DNCL”), telemarketing and the use of automatic dialling-announcing devices. Under Canada’s Do-Not-Call List Rules (“DNCL Rules”), an individual may register his or her telephone or fax number on the National DNCL to indicate that he or she does not wish to receive unsolicited telemarketing communications. In general, organisations are prohibited from placing unsolicited telemarketing calls (telephone
or fax) to numbers registered on the National DNCL unless express consent has been obtained directly from the individual in the manner prescribed under the DNCL Rules. Under the CRTC Telemarketing Rules, an organisation must maintain its own internal Do-Not-Call List and must not initiate telemarketing telecommunications to an individual on its own list.

Postal marketing communications are not specifically regulated, but must comply with the requirements of Canadian Privacy Statutes.

9.3 Do the restrictions noted above apply to marketing sent from other jurisdictions?

Yes, they do apply.

9.4 Is/are the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?

Yes. The Canadian privacy regulatory authorities have issued multiple reports of findings related to secondary marketing practices. The CRTC is also active in enforcing the Unsolicited Telecommunications Rules. Canada’s anti-spam legislation (“CASL”) came into force on July 1, 2014. The CRTC has been actively enforcing CASL and has completed dozens of investigations since then.

9.5 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?

It is only lawful if the individuals on the list were clearly and accurately informed at the point of collection about how their addresses would be used and if they consented to having their email addresses collected and used for marketing purposes. In addition, they must be able to opt out of receiving messages at any time in the future.

9.6 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?

Under Canadian Privacy Statutes, there are no specific penalties related to the unlawful sending of marketing communications. However, organisations may be subject to a complaint and investigation. In Alberta, British Columbia and Québec, an investigation may be elevated to a formal inquiry resulting in an order. Failure to comply with an order can result in fines of up to $100,000 in Alberta and British Columbia. In Alberta and Québec, organisations can also be subject to fines for failure to comply with the relevant requirements of the Acts of up to $100,000 in Alberta and $10,000 in Québec for a first offence and $20,000 for a subsequent offence.

The CRTC has the legislative authority under the Telecommunications Act to impose administrative monetary penalties for violation of the Unsolicited Telecommunications Rules. The maximum administrative monetary penalty for each violation of the Unsolicited Telecommunications Rules is $15,000 for a corporation. A violation that continues for more than one day constitutes a separate violation for each day that it is continued. In addition, a person that contravenes any prohibition or requirement of the Commission related to the Unsolicited Telecommunications Rules may be guilty of an offence punishable on summary conviction and liable, in the case of a corporation, to a fine not exceeding $100,000 for a first offence or $250,000 for a subsequent offence. There is also a limited private right of action that allows a person to sue for damages that result from any act or omission that is contrary to the Telecommunications Act or a decision or regulations.

The CRTC is also the agency primarily responsible for regulatory enforcement of CASL’s commercial electronic message provisions. CASL permits the CRTC to impose administrative monetary penalties of up to $1 million per violation for individuals and $10 million for businesses. CASL outlines a range of factors to be considered in assessing the penalty amount, including the nature and scope of the violation. CASL also sets forth a private right of action permitting individuals to bring a civil action for alleged violations of CASL ($200 for each contravention, up to a maximum of $1 million each day, for a violation of the provisions addressing unsolicited electronic messages).

10 Cookies

10.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).

There are no specific restrictions with respect to cookies under Canadian Privacy Statutes. As with other forms of collection, use and disclosure of personal information in the course of commercial activities, cookies are subject to the general requirements of Canadian Privacy Statutes.

Under Canadian Privacy Statutes, implied consent can be relied upon for the collection and use of personal information through cookies to the extent that the personal information involved is non-sensitive in nature and that it accords with the reasonable expectations of individuals.

The Privacy Commissioner of Canada’s regulatory guidance on Online Behavioural Advertising affirmed that implied (or opt-out) consent is reasonable for the purposes of online behavioural advertising provided that:

- individuals are made aware of the purposes for the practice in a manner that is clear and understandable;
- individuals are informed of these purposes at or before the time of collection and provided with information about the various parties involved in online behavioural advertising;
- individuals are able to easily opt out of the practice at or before the time the information is collected;
- the opt-out takes effect immediately and is persistent;
- the information collected and used is limited, to the extent practicable, to non-sensitive information; and
- information collected and used is destroyed as soon as possible, or effectively de-identified.

If, however, the personal information collected and used is sensitive in nature, express consent is required.

10.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?

Although there are no explicit legislative restrictions with respect to cookies specifically, the Office of the Privacy Commissioner of Canada (“OPC”) has restricted the following uses:

The first is in respect of zombie cookies, supercookies, third-party cookies that appear to be first-party cookies, device fingerprinting and other techniques that cannot be controlled by individuals. Where a tracking technique offers no option for user control, and
10.3 To date, has/have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?

Yes. The OPC has issued several reports of findings in cases involving cookies in the context of online behavioural advertising. As examples, one case involved sensitive health information (PIPEDA Report of Findings #2014-001), and the other involved a website aimed at children (PIPEDA Report of Findings #2014-011).

10.4 What are the maximum penalties for breaches of applicable cookie restrictions?

Under Canadian Privacy Statutes, there are no specific penalties related to cookie restrictions. However, organisations may be subject to a complaint and investigation under Canadian Privacy Statutes. In Alberta and British Columbia, an investigation may be elevated to a formal inquiry resulting in an order. Failure to comply with an order can result in fines of up to $100,000. In Alberta and Québec, organisations can also be subject to fines for failure to comply with the relevant requirements of the Acts of up to $100,000 in Alberta, and $10,000 in Québec for a first offence and $20,000 for a subsequent offence.

11 Restrictions on International Data Transfers

11.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.

Under Canadian Privacy Statutes governing the private sector, organisations are responsible for personal information in their custody or control, including personal information transferred to third parties for processing. In general, Canadian Privacy Statutes permit the non-consensual transfer of personal information to third-party processors outside Canada, provided the transferring organisation uses contractual or other means to provide a comparable level of protection while the information is being processed by the foreign processor.

In Alberta, more specifically, if an organisation uses a service provider outside Canada to collect, use, disclose or store personal information, the organisation must specify, in its privacy policies and practices, the foreign jurisdictions in which the collection, use, disclosure or storage is taking place, and the purposes for which the foreign service provider has been authorised to collect, use or disclose personal information on its behalf.

11.2 Please describe the mechanisms businesses typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).

Typically, companies enter into an agreement when transferring data outside of Canada for processing purposes, to ensure that the data transferred are afforded a comparable level of protection to that under Canadian Privacy Statutes. Depending on the size and the context of the data transfer arrangement in question, there are a number of measures that companies take to establish an appropriate vendor management framework, including: (i) due diligence, in particular with respect to security safeguards; (ii) contractual arrangements setting out requisite controls and conditions; (iii) appropriate notice to employees or consumers; and (iv) appropriate monitoring of the service provider arrangement. While consent is not required, notification is.

11.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.

Transfers of personal data to other jurisdictions do not require registration/notification or prior approval from the relevant data protection authorities.

12 Whistle-blower Hotlines

12.1 What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?

Under Canadian Privacy Statutes, a whistle-blower who has reasonable grounds to believe that a provision of the relevant statute has been, or will be, contravened may notify the data protection authority and request that his or her identity be kept confidential. The data protection authority shall keep confidential the person’s identity and the information he or she relayed, accordingly. The statutes further prohibit employers from taking retaliatory action against an employee who, acting in good faith and on the basis of reasonable belief, disclosed such information to the data protection authority. Any employer who knowingly contravenes this prohibition is guilty of an offence and may be subject to a fine.

12.2 Is anonymous reporting prohibited, strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do businesses typically address this issue?

Anonymous reporting is not prohibited or discouraged under Canadian Privacy Statutes. As a matter of practice, anonymous reporting of facts that are credible and can be independently verified may proceed as a Commissioner-initiated complaint if there are reasonable grounds to believe that an investigation is warranted.
13 CCTV

13.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?

The use of CCTV does not require separate registration/notification or prior approval from the relevant data protection authorities. However, as best practice in some jurisdictions, and as a matter of policy in others, organisations must conduct a privacy impact assessment and seek input from the relevant data protection authority before introducing the use of CCTV.

Appropriate and clear notice should be provided to individuals prior to the collection of personal information through video surveillance. This notice should include the purposes of the video surveillance and contact information in case the individual has questions or wishes to request access to his or her images.

13.2 Are there limits on the purposes for which CCTV data may be used?

The use of CCTV must only be for purposes that a reasonable person would consider to be appropriate in the circumstances. For instance, the use of CCTV to ensure the protection of company assets that have come under threat of being damaged or stolen, or the safety of customers in situations that have proven to be demonstrably dangerous, may be considered reasonable. On the other hand, using CCTV to generally monitor employee performance, in the absence of any prior concerns having been raised or any suspected wrongdoing, may not be.

14 Employee Monitoring

14.1 What types of employee monitoring are permitted (if any), and in what circumstances?

Employee monitoring would be permissible (both in the workplace and otherwise), provided that it is conducted in conformity with the principles under Canadian Privacy Statutes. In particular, the monitoring must be conducted for a purpose consistent with what a reasonable person would consider appropriate in the circumstances. Canadian privacy regulatory authorities generally use a four-part test to assist in determining the reasonableness of employee monitoring:

- Is the surveillance demonstrably necessary to meet a specific need?
- Is the measure likely to be effective in meeting that need?
- Is the loss of privacy proportional to the benefit gained?
- Is there a less privacy-invasive way that the employer could achieve the same end?

14.2 Is consent or notice required? Describe how employers typically obtain consent or provide notice.

Canadian Privacy Statutes governing the private sector generally allow for the collection, use and disclosure of employee personal information without consent if it is solely for the purposes reasonably required to establish, manage or terminate an employment relationship between the organisation and that individual.

While the statutes allow for the collection of personal information without consent, within the bounds of reasonableness, they nonetheless require the employer to be transparent about it; accordingly, organisations must notify employees that it is occurring, and explain the purpose(s) for the collection (such as employee safety).

Employers typically provide notice about video surveillance or monitoring upon entry to the workplace area under surveillance or upon use of the technology being monitored. Employers also implement video surveillance and monitoring policies and reference such activities in relevant privacy statements.

14.3 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?

There is no express requirement to notify trade unions regarding the use of employee monitoring under Canadian Privacy Statutes.

15 Data Security and Data Breach

15.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?

Canadian Privacy Statutes contain specific provisions relating to the safeguarding of personal information. In essence, these provisions require organisations to implement reasonable technical, physical and administrative measures to protect personal information against loss or theft, as well as unauthorised access, disclosure, copying, use, modification or destruction. The security safeguards must be appropriate to the sensitivity of the information, such that, the more sensitive the information, the higher the level of protection that will be required.

An organisation is responsible for protecting personal information in its possession or custody, including information that has been transferred to a third party for processing. They must ensure a comparable level of protection through contractual or other means.

15.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

The Federal private sector privacy law, PIPEDA, was amended in 2015 to include new breach notification requirements that came into force on November 1, 2018. With these provisions in force, PIPEDA now requires organisations to report to the Privacy Commissioner any breach of security safeguards involving personal information under its control if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to an individual. The report must be made in the prescribed form and manner, and provided as soon as feasible after the organisation determines that the breach has occurred. Reports to the Commissioner must include the following:

- a description of the circumstances of the breach and, if known, the cause;
- the day on which, or the period during which, the breach occurred or, if neither is known, the approximate period;
c. a description of the personal information that is the subject of the breach to the extent that the information is known;

d. the number of individuals affected by the breach or, if unknown, the approximate number;

e. a description of the steps that the organisation has taken to reduce the risk of harm to affected individuals that could result from the breach, or to mitigate that harm;

f. a description of the steps that the organisation has taken or intends to take to notify affected individuals of the breach; and

g. the name and contact information of a person who can answer, on behalf of the organisation, the Commissioner’s questions about the breach.

Moreover, the new breach provisions in PIPEDA require organisations to keep records, in prescribed form, of every breach of security safeguards involving personal information under its control, and to provide the Commissioner with a copy of such records on request.

Under PIPA Alberta, an organisation is required to provide notice to the Commissioner, without unreasonable delay, of a breach where there is a real risk of significant harm to individuals. Notice to the Commissioner must be in writing and include similar details to those that will be required under PIPEDA (outlined above).

15.3 Is there a legal requirement to report data breaches to affected data subjects? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

As of November 1, 2018, PIPEDA’s breach notification provisions require an organisation to notify affected individuals of a breach of security safeguards if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to the individual. The notification must be given as soon as feasible after the organisation determines that the breach has occurred. It must be conspicuous and given directly to the individual in the manner prescribed by the regulations. Indirect notification is also permissible in circumstances where direct notification is likely to cause further harm to the affected individual or undue hardship for the organisation, or where the organisation does not have contact information for the affected individual.

The contents of the notification to individuals must include:

a. a description of the circumstances of the breach;

b. the day on which, or period during which, the breach occurred or, if neither is known, the approximate period;

c. a description of the personal information that is the subject of the breach to the extent that the information is known;

b. a description of the steps that the organisation has taken to reduce the risk of harm that could result from the breach;

c. a description of the steps that affected individuals could take to reduce the risk of harm that could result from the breach or to mitigate that harm; and

d. contact information that the affected individual can use to obtain further information about the breach.

Under PIPEDA, when notice is given to individuals, it must also be given to any other organisation or government institution if the notifying organisation believes that the other organisation or the government institution may be able to reduce the risk of harm or mitigate that harm.

Under PIPA Alberta, the Commissioner, once notified, may subsequently require organisations to notify affected individuals directly of the loss or unauthorised disclosure, unless the Commissioner determines that direct notification would be unreasonable in the circumstances. Such notification must include certain elements which are similar to those that will be required under PIPEDA (above).

While other Canadian private sector data protection statutes do not contain any express data breach notification requirements, Commissioners’ findings and other guidance documents suggest that a duty to notify affected individuals is an implicit part of the general safeguarding requirements in circumstances where material harm is reasonably foreseeable, and such notification would serve to protect personal information from further unauthorised access, use or disclosure.

15.4 What are the maximum penalties for data security breaches?

Under PIPEDA, failure to comply with the breach notification provisions is (as of November 1, 2018) an offence under the Act punishable on summary conviction, liable to a fine not exceeding $10,000, or an indictable offence liable to a fine not exceeding $100,000.

Under PIPA Alberta, a failure to notify the Commissioner in the event of a breach is an offence. A person who commits an offence is liable, in the case of an individual, to a fine not exceeding $10,000, and in the case of a person other than an individual, to a fine not exceeding $100,000.

16 Enforcement and Sanctions

16.1 Describe the enforcement powers of the data protection authority(ies).

Powers of Investigation

Under PIPEDA, the Federal Privacy Commissioner shall investigate a complaint made by an individual, subject to a discretion to decline or discontinue complaints in certain circumstances.

The Federal Privacy Commissioner can also initiate an investigation based on reasonable grounds to believe that a matter warrants it. In the course of an investigation, the Commissioner has substantial powers, including the power to summon witnesses to give oral or written evidence, inspect documents and/or compel the production thereof, and inspect premises other than a dwelling house.

Under PIPA Alberta and PIPA BC, the Commissioners have similar powers of investigation. However, where a matter is not otherwise resolved, an investigation may be elevated to a formal inquiry.

Powers of Enforcement

Upon concluding an investigation under PIPEDA, the Privacy Commissioner issues a report of findings and, if applicable, recommendations for compliance. Although the report is non-binding in nature, it may be made public at the discretion of the Privacy Commissioner if it is in the public interest.

The complainant or the Commissioner, with the individual’s consent, may apply to the Federal Court for a de novo hearing. The Court has broad remedial powers to order correction of the organisation’s practices and award damages to the complainant, including damages for any “humiliation” suffered.

The OPC and the organisation may agree to enter into a voluntary compliance agreement whereby the organisation undertakes to comply with the recommendations made and bring itself into compliance with PIPEDA.
When a compliance agreement is entered into, the Commissioner shall not apply to the Court for a hearing or shall suspend any pending court application, unless or until there is breach of the agreement. If an organisation fails to live up to its commitments in a compliance agreement, the OPC could, after notifying the organisation, apply to the Court for an order requiring the organisation to comply with the terms of the agreement.

In Alberta and British Columbia, an inquiry may result in an enforceable order. Organisations are required to comply with the order within a prescribed time period, unless they apply for judicial review. In Alberta, the order may be filed with the Court and becomes enforceable as a judgment. Once an order is final, an affected individual has a cause of action against the organisation for damages for loss or injury that the individual has suffered as a result of the breach.

Similarly, in Québec, an order must be obeyed within a prescribed time period. An individual may appeal to the judge of the Court of Québec on questions of law or jurisdiction with respect to a final decision.

Audits
The OPC and the OIPC BC have the express authority to audit the personal information practices of an organisation upon reasonable grounds that the organisation is contravening the Act. The results of the audit are made public.

Offences / Criminal Sanctions
In Québec, Alberta and British Columbia, there are certain statutory provisions which, if violated, could constitute an offence and result in fines of up to $10,000 for a first offence and $20,000 for a subsequent offence in Québec, and $100,000 for an offence in Alberta and British Columbia. This includes the offence of failing to comply with an order made by the Commissioner.

Under PIPEDA, there are more limited statutory provisions, the contravention of which may result in criminal sanctions. For example, any person who knowingly destroys personal information that is the subject of an access to personal information request, retaliates against a whistle-blowing employee, obstructs the Commissioner in the course of a complaint investigation, uses deception or coercion to collect personal information in contravention of the Act, or (as of November 1, 2018) fails to notify in the event of a breach, is guilty of an offence and liable to a fine of $10,000 for an offence punishable on summary conviction or $100,000 for an indictable offence.

Data-Sharing Arrangements
The Privacy Commissioner of Canada has the express authority under PIPEDA to enter into data-sharing arrangements with provincial or foreign counterparts, as considered appropriate, to coordinate their Office’s activities (including investigations) and ensure that personal information is protected in as consistent a manner as possible.

16.3 Describe the data protection authority’s approach to exercising those powers, with examples of recent cases.

Canada has one of the most active privacy regulatory enforcement arenas in the world. The OPC and the provincial privacy regulatory authorities in the provinces of Alberta and British Columbia have been actively focused on the early resolution of individual complaints wherever possible, in order to redirect limited resources to the investigation of novel, precedent-setting complaints that raise large, systemic issues particularly in the online world (including complaints against companies such as Facebook and Google).

There has also been an increasing trend of Canadian privacy regulatory authorities initiating investigations of their own accord. The OPC, in particular, is adopting a deliberate strategy of proactive enforcement through formal, Commissioner-initiated investigations, as well as active participation in the less formal, online privacy sweeps of the Global Privacy Enforcement Network (“GPEN”).

The OPC is also collaborating more frequently with its national and international counterparts, to conduct joint investigations in accordance with formal written arrangements (e.g., Ashley Madison and WhatsApp).

Canadian privacy regulators actively pursue softer compliance tools as well, such as guideline development, public education and research on a range of emerging privacy issues – both individually and jointly – to encourage compliance up-front before problems arise.

16.4 Does the data protection authority ever exercise its powers against businesses established in other jurisdictions? If so, how is this enforced?

Although PIPEDA is silent with respect to its territorial reach, the Federal Court of Canada has found that PIPEDA will apply to businesses established in other jurisdictions if there is a “real and substantial connection” between the organisation’s activities and Canada. For instance, with respect to websites, the relevant connecting factors include: (1) where promotional efforts are being targeted; (2) the location of end-users; (3) the source of the content on the website; (4) the location of the website operator; and (5) the location of the host server.

17 E-discovery / Disclosure to Foreign Law Enforcement Agencies

Although the language varies across the statutes, under Canadian Privacy Statutes, there is generally an exception to the consent requirement when disclosing information (i) to comply with the rules of court relating to the production of records, and (ii) where required by law.

When disclosing personal information in either of these contexts, the remaining requirements under Canadian Privacy Statutes still apply. As such, organisations must only disclose the personal information in the manner and to the extent to which a reasonable person would consider appropriate in the circumstances, must limit the amount of personal information that is disclosed to that which is reasonably necessary in the circumstances, and must appropriately safeguard the transmission of personal information.

The OPC also expects organisations to be open and transparent when transferring data across borders, in particular by openly notifying individuals that personal information transferred to another jurisdiction becomes subject to foreign laws and may be accessed by the courts, law enforcement and national security authorities in those jurisdictions.
17.2 What guidance has/have the data protection authority(ies) issued?

The OPC has released a guidance document entitled *Guidelines for Processing Personal Data Across Borders*, which addresses lawful access by foreign authorities.

The OPC has also released a guidance document entitled *PIPEDA and Your Practice: A Privacy Handbook for Lawyers*, which addresses privacy issues associated with e-discovery.

18 Trends and Developments

18.1 What enforcement trends have emerged during the previous 12 months? Describe any relevant case law.

See question 16.3 above for a description of the more proactive enforcement trends that have emerged during recent years, including the previous 12 months.

In terms of relevant case law, courts continue to refine the contours of common law privacy torts, including the tort of invasion of privacy and the tort of publication of embarrassing private facts.

Also, this past year, in *R. v. Reeves, 2018 SCC 56*, the Supreme Court of Canada found a reasonable expectation of privacy in shared personal computers, and in *R. v. Jarvis, 2019 SCC 10*, the Supreme Court of Canada found that there can be a reasonable expectation of privacy in public places for the purpose of enforcing voyeurism provisions of the Criminal Code of Canada.

18.2 What “hot topics” are currently a focus for the data protection regulator?

Canada’s Federal Privacy regulator, the OPC, has established four strategic privacy priorities to guide the Office’s discretionary work through 2020: economics of personal information; government surveillance; reputation and privacy; and the body as information.

The Office is currently focused on its new Guidelines for Obtaining Meaningful Consent, which it released in May 2018 and began applying as of January 1, 2019, and on PIPEDA’s new data breach reporting requirements, which came into force on November 1, 2018.

The OPC continues to focus on national security reforms in Canada and the interplay with data protection. The Office has not finalised its policy position on the right to be forgotten in Canada, having initiated a Federal Court proceeding in October 2018 to seek clarity on whether Google is subject to PIPEDA when it indexes web pages and displays search results in response to searches of a person’s name. The OPC continues to shift its focus towards more proactive enforcement of broad systemic issues in collaboration with its national and international counterparts.

Canadian privacy regulators are increasingly interested in the role that ethics should play in the effective governance of big data, analytics and artificial intelligence initiatives. There is also an active interest on the part of Canadian regulators to pursue the growing intersection between data protection, competition and consumer protection law, and a recognition of the corresponding need for increased collaboration between them.

The CRTC continues to actively enforce the commercial electronic message provisions in CASL. The CRTC has entered into six undertakings regarding potential CASL violations that included payments to the CRTC ranging from $10,000 to $200,000, and has made three compliance and enforcement decisions, with administrative monetary penalties ranging from $15,000 to $200,000.
Adam Kardash
Osler, Hoskin & Harcourt LLP
100 King Street West
1 First Canadian Place
Suite 6200, P.O. Box 50
Toronto ON M5X 1B8
Canada
Tel: +1 416 862 4703
Email: akardash@osler.com
URL: www.osler.com

Adam is an acknowledged Canadian legal industry leader in privacy and data management; he co-leads Osler’s national Privacy and Data Management Group. Adam has been lead counsel on many of the most significant privacy matters in Canada. He advises Fortune 500 clients in their business-critical data protection issues, compliance initiatives and data governance. He regularly represents clients on regulatory investigations and security breaches.

Adam is Special Counsel to the Interactive Advertising Bureau of Canada and Counsel to the Digital Advertising Alliance of Canada. He has extensive experience in the privacy law area and regularly advises Chief Privacy Officers, in-house counsel and compliance professionals in the private, health, public and not-for-profit sectors on managing security incidents, privacy regulatory investigations, anti-spam law compliance, privacy and security reviews/audits, privacy policies, practices and procedures, privacy compliance initiatives, and service provider arrangements involving personal information, including trans-border data flows.

For further information, please visit https://www.osler.com/en/team/adam-kardash.

Patricia Kosseim
Osler, Hoskin & Harcourt LLP
Suite 1900
340 Albert Street
Ottawa ON K1R 7Y6
Canada
Tel: +1 613 787 1008
Email: pkosseim@osler.com
URL: www.osler.com

Patricia is Counsel in Osler’s Privacy and Data Management Group and Co-Leader of Osler’s AccessPrivacy© platform. Patricia is a national leading expert in privacy and access law, having served over a decade as Senior General Counsel at the Office of the Privacy Commissioner of Canada (OPC). There she: provided strategic legal and policy advice on complex privacy issues; advised Parliament on privacy implications of legislative bills; led research initiatives on emerging information technologies; and advanced privacy law in major litigation cases before the courts, including the Supreme Court of Canada.

Previously, Patricia worked at Genome Canada and the Canadian Institutes of Health Research, where she developed and led national strategies for addressing legal, ethical and social implications of science and technology. Patricia began her career in Montréal, practising in the areas of health law, privacy law, civil litigation, and labour and employment with another leading national law firm. She has published and spoken extensively on matters of privacy law, health law and ethics.

For further information, please visit https://www.osler.com/en/team/patricia-kosseim.

Osler is a leading business law firm advising Canadian and international clients from offices across Canada and in New York. With well over 400 lawyers, the firm is recognised for the breadth and depth of its practice and is consistently ranked as one of Canada’s top firms in national and international surveys. Osler has the largest team of practitioners who focus exclusively on privacy and data management in Canada, providing expert legal advice on increasingly complex issues.

Osler’s AccessPrivacy© provides an integrated suite of innovative information solutions, consulting services and thought leadership. The AccessPrivacy© platform helps organisations in the public, private and not-for-profit sectors navigate the complex regulatory environment and develop a strategic approach to privacy and information management, supported by sound policies and practices.
Chapter 11

Chile

Rossi Asociados

Claudia Rossi

1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?
The principal data protection legislation is Law 19.628 on the protection of personal life (also referred to herein as the Law).

1.2 Is there any other general legislation that impacts data protection?
Yes. The Chilean Constitution, in its Article 19 Nos. 4 and 5, sets forth and guarantees the right of privacy. Also, the Consumer Protection Law (Law 19.496) establishes rules on unsolicited commercial or marketing communications sent to consumers.

1.3 Is there any sector-specific legislation that impacts data protection?
Yes. Health, labour, telecommunications, financial, banking and commercial laws impact data protection.

1.4 What authority(ies) are responsible for data protection?
The Council for Transparency is responsible for ensuring the compliance of public entities with Law 19.628, but there is no regulatory authority that monitors compliance with data privacy laws by the private sector.

2 Definitions

2.1 Please provide the key definitions used in the relevant legislation:

- “Personal Data”
  This is defined as data concerning identified or identifiable natural persons.

- “Processing”
  This is defined as any operation or complex set of operations or technical processes, automated or not, that allows the collecting, storing, recording, organising, devising, selecting, extracting, confronting, interconnecting, dissociating, communicating, assigning, transferring, or cancelling of personal data, or the use of it in any other way.

- “Controller”
  This is not applicable.

- “Processor”
  This is defined as the natural person or legal private entity, or the respective public body, which is responsible for making decisions related to personal data processing.

- “Data Subject”
  This is defined as the individual to whom the personal data refer.

- “Sensitive Personal Data”
  This is defined as personal data referring to individuals’ physical or moral characteristics or to facts or circumstances of their private life or intimacy, such as personal habits, racial origin, ideologies and political opinions, religious beliefs or convictions, physical or mental health, and sexual life.

- “Data Breach”
  This concept is not defined by current legislation.

Other key definitions – please specify (e.g., “Pseudonymous Data”, “Direct Personal Data”, “Indirect Personal Data”)

- “Obsolete Data”
  This is defined as that which has lost its relevance in law by means of the fulfilment of the condition or the expiration of the term set forth for its validity or, in the absence of any specific law regulating this, the change of facts or circumstances covered by it.

- “Statistical Data”
  This is defined as data that, in its origin or as a result of its processing, cannot be associated with an identified or identifiable subject.

- “Sources Accessible to the Public”
  This is defined as personal data registers or compilations, public or private, whose access is not restricted or reserved for applicants.

- “Registry or Data Bank”
  This is defined as an organised set of personal data, automated or not, and its form or the method of its creation or organisation, that allows for the comparison of data, as well as the facilitation of data processing.
3 Territorial Scope

3.1 Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to those laws?

This concept is not defined by current legislation.

4 Key Principles

4.1 What are the key principles that apply to the processing of personal data?

- Transparency
  There is no application of this principle in Law 19.628. There is only a very specific obligation on the Bureau of Credit, according to Law 20.575, stating that it must designate a person that is in charge of the treatment of data; therefore, data subjects can ask him or her to ensure or enforce their rights.

- Lawful basis for processing
  According to Article 1 of the Law, the processing shall be made:
  - in a manner consistent with the law;
  - for the purposes allowed by the legal system; and
  - with respect to the full exercise of the data subjects’ fundamental rights and facilities granted to them by the Act.

- Purpose limitation
  This principle is applied:
  - as one of the conditions that the processing must comply with;
  - as information to be provided to the data subject, at the moment of collection of its data, in order to process it;
  - as a condition for the use of personal data by those who are responsible for data records and distributors of records; and
  - as part of the right of access and information.

  Personal data shall be used only for the purpose for which they were collected, unless they are obtained from sources accessible to the public (Article 9 of the Law).

- Data minimisation
  There is no application of this principle in Law 19.628.

- Proportionality
  There is no application of this principle in Law 19.628.

- Retention
  There is no application of this principle in Law 19.628.

Other key principles – please specify

- Quality
  Article 6 of the Law states that personal data shall be: destroyed or cancelled when the purpose for their storage lacks legal basis or when it has expired; modified when they are erroneous, inexact, misleading, or incomplete; and blocked when they cannot be destroyed or cancelled, and their accuracy cannot be established or their validity is doubtful.

  The person responsible for the database must eliminate, modify, or block the data, as stated above, without mandatory notification of the data subject.

- Data subject consent
  Article 4 of the Law states that the processing of personal data is permitted only when the law authorises it, or the data subject expressly consents to it or authorises it. However, the Law does not provide a definition of what the “authorisation” or “consent” of the data subject means or entails.

- Security of the data
  Article 11 of the Law provides that those responsible for the registries or personal databases must “take care of them with due diligence” and are liable for damages.

- Confidentiality of the data
  Article 7 of the Law sets forth that people who work on processing personal data, in the public and private sectors, are required to maintain confidentiality about them, when they come from sources not accessible to the public, as well as regarding other data and information related to the data bank; an obligation that does not cease upon termination of their functions or activities in that field.

- Specially protected personal data
  Article 10 of the Law prescribes that sensitive personal data cannot be processed unless (i) the law authorises it, (ii) the data subject agrees expressly to such processing, or (iii) such data are necessary for establishing or granting health benefits that pertain to the respective data subject.

5 Individual Rights

5.1 What are the key rights that individuals have in relation to the processing of their personal data?

- Right of access to data/copies of data
  The right pertaining to all data subjects to demand from the person responsible for any public or private data bank information pertaining to him, its source, the purpose of collection, the lawfulness of the data processing, and the name of the individuals or entities to which the data are regularly transmitted.

- Right to rectification of errors
  Article 12 of Law 19.628 establishes that if the data content in any data bank (private or public) is proven false, inaccurate, incorrect or incomplete, data subjects have the right to demand the rectification of those errors.

- Right to deletion/right to be forgotten
  This right is not currently protected by the Law.

- Right to object to processing
  There is no general right of opposition recognised by law; it is limited to certain cases. The data subject is only entitled to exercise this right in three cases: for advertising purposes; for market surveys; or for opinion polls.

- Right to restrict processing
  This right is not currently protected by the Law.

- Right to data portability
  This right is not currently protected by the Law.

- Right to withdraw consent
  Law 19.628 establishes that data subjects always have the right to demand the rectification, elimination or cancellation of their data content in public or private data banks, unless those activities involve affecting the performance of auditing authorities, legal secrets, national security or the national interest.

- Right to object to marketing
  Article 28 B of the Consumer Protection Law (Law 19.496) regulates unsolicited commercial or marketing communications sent via email to consumers, specifying that such communication must contain a valid email address to which the recipient can request the suspension of further communications (opt-out).
Rights to complain to the relevant data protection authority(ies)

Considering that a data protection authority does not exist in Chile, the only way to complain about the illegal treatment of personal data is through a jurisdictional action in court. To this end, Law 19.628 establishes a special procedure named “habeas data”. Nevertheless, it is usual practice for the data subject to use, in addition, the “Recurso de Protección”, a constitutional action, in order to protect his or her fundamental rights affected by an illegal or arbitrary treatment of personal data.

Other key rights – please specify

- **Blocking**
  The right of the data subject to request temporary suspension of any data processing activity when data accuracy cannot be established, or its validity is doubtful, and as long as such personal data cannot be cancelled.

6 Registration Formalities and Prior Approval

6.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?

This obligation does not exist or apply, since there is no authority that regulates the registration of data held by private companies.

6.2 If such registration/notice is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?

This is not applicable.

6.3 On what basis are registrations/notices made (e.g., per legal entity, per processing purpose, per data category, per system or database)?

This is not applicable.

6.4 Who must register with/notify the data protection authority (e.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation)?

There is no obligation for registration or notification.

6.5 What information must be included in the registration/notice (e.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes)?

There is no obligation for registration or notification.

6.6 What are the sanctions for failure to register/notify where required?

This is not applicable.

6.7 What is the fee per registration/notice (if applicable)?

This is not applicable.

6.8 How frequently must registrations/notifications be renewed (if applicable)?

This is not applicable.

6.9 Is any prior approval required from the data protection regulator?

This is not applicable.

6.10 Can the registration/notice be completed online?

This is not applicable.

6.11 Is there a publicly available list of completed registrations/notifications?

This is not applicable.

6.12 How long does a typical registration/notice process take?

This is not applicable.

7 Appointment of a Data Protection Officer

7.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.

Chilean law does not regulate or establish a Data Protection Officer or any other similar body; therefore, there is no requirement to comply with this issue.

7.2 What are the sanctions for failing to appoint a Data Protection Officer where required?

This is not applicable.

7.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect of his or her role as a Data Protection Officer?

This is not applicable.

7.4 Can a business appoint a single Data Protection Officer to cover multiple entities?

This is not applicable.
7.5 Please describe any specific qualifications for the Data Protection Officer required by law.

This is not applicable.

7.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?

This is not applicable.

7.7 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?

This is not applicable.

7.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?

This is not applicable.

8 Appointment of Processors

8.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?

Article 7 of Law 19.678 points out that people who work in the processing of personal data, both in public and private organisations, are obliged to keep them secret, when they come from or have been collected from sources not accessible to the public. To enforce the aforementioned obligation, companies enter into agreements with the persons who may be in charge of processing the information for which they are responsible.

8.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?

Although the law does not establish the obligation to enter into an agreement, its purpose is to comply with article 7 of Law 19.678. The agreement is contractual in nature and therefore its content is determined by the autonomy of the will of the parties.

9 Marketing

9.1 Please describe any legislative restrictions on the sending of electronic direct marketing (e.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?).

According to Article 4 of the Law, an authorisation from the data subject is not required for the collection of personal data from sources accessible to the public if such data are necessary for commercial communications of direct response or direct marketing of goods and services. In any case, the Consumer Protection Law (Law 19.496) establishes rules on the protection of consumer rights, particularly when referring to unsolicited commercial or marketing communications sent to consumers. Article 28 B of this Law regulates unsolicited commercial or marketing communications sent via email to consumers, specifying, among other things, that such communication must contain a valid email address to which the recipient can request the suspension of further communications, otherwise referred to as an opt-out system. From the moment that the recipient requests the suspension of sending further emails, any communication or unsolicited email is forbidden by law.

9.2 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.).

There is no legislation that restricts the aforementioned practice.

9.3 Do the restrictions noted above apply to marketing sent from other jurisdictions?

This is not applicable.

9.4 Is/are the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?

There is no data protection authority. Nevertheless, the National Consumer Service (SERNAC) is active in enforcing breaches of marketing restrictions.

9.5 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?

There is no legislation that regulates this specific matter. However, if marketing lists contain data from accessible sources, there is no restriction on its communication or sale.

9.6 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?

There is no special penalty for this breach, but a general sanction set forth in the Consumer Protection Law (Law 19.496) applies. According to Article 24 of the aforementioned law, a fine of up to 50 monthly tax units (UF) will apply in case of this type of infringement.

10 Cookies

10.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).

There is no legislation that regulates the use of cookies.

10.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?

This is not applicable.
10.3 To date, has/have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?

This is not applicable.

10.4 What are the maximum penalties for breaches of applicable cookie restrictions?

This is not applicable.

11 Restrictions on International Data Transfers

11.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.

The Law does not set forth specific requirements or restrictions on transfers of personal data abroad. The Law does not restrict transfers of personal data to third countries.

11.2 Please describe the mechanisms businesses typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).

Since there are no transfer restrictions, businesses only use the standard clause established by EU legislation, when Chilean businesses have received personal data from Europe.

11.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.

The Law contains some rules on the automated transmission of data. Article 5 of the Law prescribes that the person responsible for a registry or database can establish an automated system for the transmission of personal data, provided that it adequately guarantees the rights or interests of the parties involved, and such transmission is strictly related to the duties and objectives of the participating entities. Also, in the case of an application for the transmission of personal data through an electronic network, the following shall be recorded:

a) Identification of the requesting party.

b) Reason and purpose of the consultation.

c) Type of data transmitted.

The admissibility of the request must be examined by the entity responsible for data collection, but the requesting party is responsible for complying with the requirements. The receiving party is only authorised to use said personal data for the purposes that served as the basis for the transmission. This article does not apply when personal data is available to the general public.

12 Whistle-blower Hotlines

12.1 What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?

Chile lacks comprehensive whistle-blower laws or legal provisions to protect whistle-blowers from retaliation in both the public and private sectors.

Chilean corporate liability legislation takes into account the effectiveness of a company’s compliance programme when determining corporate liability for a crime that may have been committed during that company’s activities, or as a mitigating factor when sentencing. Law 20.393, enacted in 2009, allows corporate liability for a range of offences, including foreign bribery. Corporations can avoid or mitigate liability if they have put in place an offence prevention model in accordance with the provisions of this law. One of the required elements of an offence prevention model is a channel for reporting violations. There are no restrictions regarding personal data of the person who may submit a claim, or whom a report may concern.

Only the Labour Code’s workplace harassment provisions provide any kind of recourse for private-sector whistle-blowers who suffer retaliation for reporting.

12.2 Is anonymous reporting prohibited, strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do businesses typically address this issue?

This is not applicable.

13 CCTV

13.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?

No, it is not necessary.

13.2 Are there limits on the purposes for which CCTV data may be used?

A limitation applies when CCTV is intended to be used as evidence in a criminal proceeding. It falls to the Judge of Guarantee to authorise the exhibition of the images captured by these devices according to the Chilean Criminal Procedure Code in its articles 181, 226 and 323. Therefore, the single substantive regulation regarding the use of images captured by video cameras (CCTV) is established in criminal procedure law.

14 Employee Monitoring

14.1 What types of employee monitoring are permitted (if any), and in what circumstances?

Employers are entitled to monitor employees’ conduct and
communications in the workplace only under certain circumstances and in compliance with employees’ constitutional rights concerning intimacy, private life or honour.

Therefore, in accordance with administrative and judicial jurisprudence, employee monitoring shall only be carried out with regard to information related to the work and in compliance with the non-discrimination principle, and as long as monitoring is communicated to employees in advance. There should be a balance between employers’ rights (property right and performance of a private economic activity) and those of employees.

Even though computers at the workplace are the property of the employer, they can – and mostly do – contain information and personal data of employees. The employer can be prevented from monitoring them because it would be a violation of the employee’s privacy, unless monitoring is regulated by internal regulations at the workplace.

Further, employers can restrict the use of the internet and declare as non-private certain types of activity or communications, always allowing for an appropriate level of freedom for the employees.

14.2 Is consent or notice required? Describe how employers typically obtain consent or provide notice.

Employee consent is required if some kind of permitted monitoring is agreed in labour contracts. Notice is always required when regulating monitoring at the workplace.

14.3 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?

It is not mandatory, but it is highly advisable.

15 Data Security and Data Breach

15.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?

The Law does not establish standards of care or specific measures to take in order to ensure the security of data or prevent damage.

15.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

There are no legal requirements regarding this, as there is no data protection authority to whom breaches can be reported.

15.3 Is there a legal requirement to report data breaches to affected data subjects? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

This is not applicable (see the answer above).

15.4 What are the maximum penalties for data security breaches?

There is no specific penalty for security breaches.

16 Enforcement and Sanctions

16.1 Describe the enforcement powers of the data protection authority(ies).

<table>
<thead>
<tr>
<th>Investigatory Power</th>
<th>Civil/Administrative Sanction</th>
<th>Criminal Sanction</th>
</tr>
</thead>
<tbody>
<tr>
<td>Civil courts</td>
<td>Fine determined by the judge.</td>
<td>Not applicable.</td>
</tr>
</tbody>
</table>

16.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?

Currently, the authority in charge of data protection is the Council For the Transparency; however, it is only responsible for auditing the records kept by public bodies.

16.3 Describe the data protection authority’s approach to exercising those powers, with examples of recent cases.

This is not applicable; please see question 16.2 above.

16.4 Does the data protection authority ever exercise its powers against businesses established in other jurisdictions? If so, how is this enforced?

This is not applicable; please see question 16.2 above.

17 E-discovery / Disclosure to Foreign Law Enforcement Agencies

17.1 How do businesses typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?

This is not applicable.

17.2 What guidance has/have the data protection authority(ies) issued?

This is not applicable.

18 Trends and Developments

18.1 What enforcement trends have emerged during the previous 12 months? Describe any relevant case law.

No particular trends have emerged.
The Data Protection Bill N°11144, of presidential initiative, was introduced in March 2017, and recently consolidated with another bill that proposed similar modifications to our data protection regulation, contained in Law 19.628 on Protection of Privacy.

This bill had been held in Congress for a while since the Senate, on 22 March 2017, agreed to make some progress and decided to recast it with another bill (N°11092-07), in which similar modifications were intended in the matter of data treatment and its regulation.

Finally, on 14 March of the present year, both bills were consolidated; which resulted in one new project whose text was released to the public in April by the Constitution, Legalisation, Justice and Regulation Commission.

The Bill aims to regulate data treatment and reinforce its protection by making important adjustments to our current data protection regulation, contained in Law 19.628 on the Protection of Privacy.

The most significant changes that this bill brings to our legislation are the following:

- In the first place, the bill sets a new scope for our current data protection Law 19.628.
- It incorporates a number of terms and adjusts others that are already established in the current law. One of the most important additions is the definition and requirements of the data subject’s consent, as well as the modifications incorporated to the definition of sensitive data. The current legislation does not contemplate such a specific regulation in this matter.
- It grants every data subject the ARCO rights (access, rectification, cancellation and opposition), specifying their meaning, content and how to exercise each one of them.
- In relation to the data processing of minors, it strengthens the existing regulation in accordance with the new European General Data Protection Regulation (GDPR). It incorporates new categories of data such as biometric information and data related to the human biological profile.
- One of the most innovative changes is the creation of a data protection entity called the “Agency for the Protection of Personal Data”. This body will be in charge of ensuring compliance with the law along with the supervision and inspection of the data controllers. The faculty to sanction non-compliance with the law will apply for both public and private entities.
- To those who process personal data, it establishes the obligation to inform data subjects about the purpose of the collection of their data.
- It creates a series of rules for data transfer operations both nationally and internationally. The criterion used in this bill is that the transfer of personal data outside the national borders may be made only if the country to which the transfer is made has adequate standards of security and quality. These standards are set by the Agency for the Protection of Personal Data.

To sum up, all the amendments and guidelines proposed by this bill are intended to update and modernise the legal framework regarding data protection and resemble the GDPR as much as possible. This is because the GDPR is considered to be the most important change in data privacy regulation in 20 years and therefore a model to follow.

Current Status

Since both bills were recently consolidated into one project, there has been no further progress in the legislative process and the general discussion of the bill is now pending in the Senate. So, nothing remains but to wait for the bill to continue its way through the First Constitutional Process, and finally become our new data protection law.
1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

The principal personal data protection legislation in China is the Cybersecurity Law of the People's Republic of China (hereinafter the “CSL”). It sets out data protection requirements for network operators.

1.2 Is there any other general legislation that impacts data protection?

There is civil and criminal legislation that has an impact on data protection. In particular, the General Rules of the Civil Law became effective on 1 October 2017, in which Article 111 provides that natural persons' personal data is protected by law. Illegally collecting, using, processing or transferring the personal data of others is not allowed.

The Criminal Law also sets forth offences relating to infringing personal data and privacy, e.g., the offence of infringing citizens' personal information in Article 253-(1), the offence of refusing to fulfill information network security responsibilities in Article 286-(1), and the offence of stealing, purchasing or illegally disclosing other people’s credit card information in Article 177-(1). The Interpretation of Several Issues Regarding Application of Law to Criminal Cases of Infringement of Citizen's Personal Information Handled by the Supreme People's Court and the Supreme People's Procuratorate issued in 2017 provides further explanation regarding the offences relating to infringing personal data and privacy.

Article 2 of the Tort Liability Law sets the right to privacy as one of the civil rights of citizens, along with right to life, right to health, etc.

1.3 Is there any sector-specific legislation that impacts data protection?

There are also specific legislations in sectors of banking, insurance, medical, credit information, telecommunications and automobiles that impact data protection, such as the Implementing Measures of the People's Bank of China for the Protection of Financial Consumers’ Rights and Interests, the Measures for Administration of Population Health Information, the Medical Records Administration Measures of Medical Institutions, the Administrative Regulations on Credit Investigation Industry, the Several Provisions on Regulating the Market Order of Internet Information Services, the Measures for the Administration of Internet Email Services, and the Provisions on Protecting the Personal Information of Telecommunications and Internet Users, etc.

1.4 What authority(ies) are responsible for data protection?

China has no single authority responsible for enforcing provisions relating to the protection of personal information.

Under the CSL, the Cyberspace Administration of China (“CAC”) is responsible for the planning and coordination of cybersecurity and relevant supervisory and administrative work, while the Ministry of Industry and Information Technology, the public security department and other relevant departments are responsible for the supervision and administration of personal information protection in their respective sectors.

For example, the Ministry of Public Security (“MPS”) and its local branches are entitled to impose administrative penalties and are also in charge of criminal investigations against unlawful obtaining, sale or disclosure of personal information.

The Ministry of Industry and Information Technology and the telecommunications administrations at the provincial level are responsible for the supervision and administration of personal information in the telecommunications and internet sector.

Also, the State Administration for Market Regulation (“SAMR”) and its local counterparts are responsible for the supervision and administration of personal information of consumers, pursuant to the Law on Protection of the Rights and Interests of Consumers.

2 Definitions

2.1 Please provide the key definitions used in the relevant legislation:

- “Personal Data”
  “Personal Data”, or personal information as in Article 76-(5) of the CSL, refers to various information which is recorded in electronic or any other form and used alone or in combination with other information to identify a natural person, including but not limited to the name, date of birth, ID number, personal biological identification information, address and telephone number of the natural person.

- “Processing”
  Given that the major legislation, the CSL, only provides definitions for a few key terms, some of the definitions hereby
3 Territorial Scope

3.1 Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to those laws?

Theoretically, yes. Article 5 of the CSL grants the authorities the power to monitor, prevent and manage cybersecurity risks and threats from other jurisdictions. Pursuant to Article 50, if any information from other jurisdictions is found to be prohibited by law, the CAC and competent authorities may take measures to block the transmission of such information. Pursuant to Article 75, the law applies to an overseas institution, organisation or individual that engages in activity that endangers Critical Information Infrastructure (“CII”) too.

Further, companies operating under the offshore model but providing services to Chinese clients/users may also be subject to the personal data protection rules established by the CSL, especially those on the cross-border transfer of data.

However, the law does not clearly specify how to realise the sanctions. As such, the extent to which these provisions will be enforced abroad against overseas companies remains unclear.

4 Key Principles

4.1 What are the key principles that apply to the processing of personal data?

- Transparency
  Article 41 of the CSL stipulates that network operators shall make public the rules for collecting and using personal data, and expressly notify the purpose, methods and scope of such collection and use.

  In Section 4e), the Standard also sets out transparency as one of the basic principles, stating that the scope, purpose and rules of personal data processing should be publicly available and be clear, understandable and fair, and subject to external supervision.

- Lawful basis for processing
  Article 41 of the CSL requires the network operators to abide by the “lawful, justifiable and necessary” principles when collecting and using personal data.

  Section 5.1 of the Standard further explains what “lawful” means – data controllers shall not force, deceive or inveigle the data subject into disclosing personal data, shall not conceal that the product or service it provides collects personal data, shall not obtain personal data from illegal channels and shall not collect information prohibited by law.

  Among others, consent is the most common method for achieving lawfulness. Section 4c) of the Standard lists consent as a basic principle, which requires a personal data controller to obtain the data subjects’ permission on the purpose, methods, scope and rules, etc. of processing the data.

  It is to be noted that consent does not always equal lawfulness; Section 5.4 of the Standard further provides exceptions to the requirement of obtaining consent, where consent is not necessary prior to the collection and use of personal data. Nonetheless, be sure to bear in mind that the Standard is not an enforceable legal text, but a set of recommendations. Therefore, it is recommended to always obtain a data subject’s consent where possible.

- Purpose limitation
  Article 41 of the CSL requires that network operators shall not collect any personal data that is not related to the services it provides. In Section 4b) of the Standard, there is also the “Clear Purpose Principle”, where a data controller must have a lawful, legitimate, necessary and clear purpose of processing personal data.

- Data minimisation
  The CSL does not expressly provide requirements for data minimisation but only generally requires network operators to only collect personal data relevant and necessary for the provision of their services to data subjects.

  Section 5.2 of the Standard sets out that except as otherwise agreed with data subjects, data controllers shall only process the minimum type and amount of personal data necessary to fulfil the purpose the data subject has given consent to. After the purpose is fulfilled, the personal data should be deleted or anonymised promptly.
Individual Rights

5 Individual Rights

5.1 What are the key rights that individuals have in relation to the processing of their personal data?

■ Right of access to data/copies of data

Given that only rights to rectification and deletion are stated expressly in the CSL, some of the rights hereby listed are provided by the Standard. Section 7.4 of the Standard provides that a data controller should provide a personal data subject with access to:
1) the data or the type of data about him or her held by the controller;
2) the source(s) and the purpose of such personal data; and
3) the identity type of any third party who has obtained the above personal data.

■ Right to rectification of errors

Article 43 of the CSL provides that each individual is entitled to require any network operator to make corrections if he or she has found errors in such information collected and stored by such operator. The Standard provides similar rules in Section 7.5.

■ Right to deletion/right to be forgotten

Under Article 43 of the CSL, each individual is entitled to require a network operator to delete his or her personal data if he or she finds that the collection or use of such information by such operator violate the laws, administrative regulations or the agreement by and between such operator and him or her. Apart from the above circumstances, Section 7.6 of the Standard further provides that if the data controller shares and transfers the personal data to a third party, or publicly discloses the personal data illegally or in breach of the agreement between the controller and the subject, and the subject demands that the data be deleted, the controller should stop such sharing, transferring and publicly disclosing, and notify the relevant parties to delete the relevant data. Section 7.8 provides that data subjects shall be provided channels to close his or her account and the relevant personal data shall be deleted/anonymised. Further, Section 6.4 provides that if a personal information controller suspends operation in regard to its products or services, it shall delete or anonymise the personal information it holds.

■ Right to object to processing

Under the Standard, a data subject’s withdrawal of consent can be seen as a right to object to processing. It is to be noted that, pursuant to Section 7.10 of the Standard, a personal data subject will not be provided with a right to object but a right to appeal when decisions are made by information systems based on automated decisions (such as personal credit, loan limits or interview screening based on user profiling), which significantly influence the data subject’s rights and interests.

■ Right to restrict processing

The CSL does not provide explicitly for the right to restrict processing.

■ Right to data portability

The CSL does not provide explicitly for the right to data portability. According to Section 7.9 of the Standard, the right of data portability is of two kinds: (1) the data controller provides a copy of certain personal data to the data subject; and (2) the data controller directly sends the copy to a third party where technically feasible. The personal data which can be portable are confined into four kinds: basic personal data; personal identification information; personal health and physiology information; and personal education and occupational information.

■ Right to withdraw consent

Personal data subjects have complete freedom and control in respect of the handling of his/her personal data. Although it is not explicitly provided in the CSL, Section 7.7 of the Standard provides practical guidelines regarding the revocation and modification of consent under two different scenarios: (1) the withdrawal of consent for refusing to receive commercial advertisements; and (2) the withdrawal of consent for data sharing, transfer and public disclosure.

■ Right to object to marketing

Section 7.7 of the Standard stipulates that data subjects have the right to not receive commercial advertisements that are based on his or her personal data.

■ Right to complain to the relevant data protection authority(ies)

The right of individuals to complain to data protection authorities has been recognised in a number of pieces of legislation. For example, Section IX of the Decision of the Standing Committee of the National People’s Congress on Strengthening Network Information Protection provides that any organisation or individual has the right to report to the relevant authorities regarding the illegal or criminal conduct of stealing or otherwise unlawfully acquiring, selling or providing to others a citizen’s personal electronic information. Further, the CSL provides in Article 14 that one could report acts that endanger network security to the CAC, telecom, and public security authorities.

■ Other key rights – please specify

There are no other specific key rights.

6 Registration Formalities and Prior Approval

6.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?

There are such requirements regarding the cross-border transfer of data. In particular, network operators shall conduct security assessments on transmitting data abroad. The Measures for the Security Assessment of Personal Data and Important Data to be Transmitted Abroad (draft for comment, hereinafter “the Draft”) stipulates in Article 9 that if the data to be transferred involves any of the following circumstances, network operators shall apply to the...
Can the registration/notification be completed online?

It remains unclear whether the notification can be completed online.

How frequently must registrations/notifications be renewed?

It remains unclear whether the notification can be renewed.

Is any prior approval required from the data protection regulator?

For CII operators, it is widely recognised that a prior approval is required when transferring data abroad for business needs. Article 10 of the Draft further provides that the relevant authority or regulator shall complete the security assessment within 60 working days and shall disclose the assessment result to relevant network operators, and Article 11 sets out circumstances where data is not allowed to be transferred. This may indicate that a prior approval would be required.

What information must be included in the registration/notification (e.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes)?

Please see question 6.2 regarding the information to be included in the notification.

What are the sanctions for failure to register/notify where required?

The law does not specify the sanctions for average network operators, but Article 66 of the CSL sets out the sanctions for CII operators’ failure to seek approval from the authority. Specifically, it shall be warned and ordered to make rectifications, and shall be subjected to confiscation of illegal earnings and a fine ranging from RMB50,000 to RMB500,000, and may be subjected to suspension of a related business, winding up for rectification, shutdown of websites and revocation of business licences. The supervisor directly in charge and other directly liable persons shall be subject to a fine ranging from RMB10,000 to RMB100,000.

What is the fee per registration/notification (if applicable)?

Currently, it remains unclear. Normally, such notifications are free of charge.

6.7 How frequently must registrations/notifications be renewed (if applicable)?

Article 12 of the Draft provides that networks operators concerning international data transfer shall conduct a security assessment annually and make notifications accordingly where required.

Who must register with/notify the data protection authority (e.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation)?

Please see question 6.1 regarding who must notify the authority.
6.12 How long does a typical registration/notification process take?

Currently, there is no specific time frame for the notification. Detailed implementation measures or guidelines are expected to be formulated.

7 Appointment of a Data Protection Officer

7.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.

It is provided in Article 21 of the CSL that network operators should appoint network security officers to protect the security of the network. Further, it is provided in Article 34 that a CII operator shall also appoint a security management officer. The appointments of such officers are mandatory. And Section 10.1 of the Standard specifies that the personal data controller shall appoint a Data Protection Officer and set up a Data Protection Department.

7.2 What are the sanctions for failing to appoint a Data Protection Officer where required?

Since the appointment of a Data Protection Officer is a good practice to follow, set by the Standard, there is no sanction for failing to do so under the CSL. Nonetheless, there are sanctions for failure to appoint a network security officer, and in case of a CII operator, a security management officer too, under Article 59 of the CSL.

Operators that fail to appoint a network security officer can expect warnings and orders for rectifications. A fine ranging from RMB10,000 to RMB100,000 may be imposed if the operator refuses to make rectifications or in case of consequential severe damage. A fine ranging from RMB5,000 to RMB50,000 may be imposed on the person directly in charge.

CII operators that fail to appoint a security management officer can expect warnings and orders for rectifications. A fine ranging from RMB100,000 to RMB100 million may be imposed if the operator refuses to make rectifications or in case of consequential severe damage. A fine ranging from RMB10,000 to RMB100,000 may be imposed on the person directly in charge.

7.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect of his or her role as a Data Protection Officer?

If a Data Protection Officer failed to perform his or her duty with due diligence, then he or she may be accused of administrative or even criminal liabilities in respect to his or her role as a Data Protection Officer.

7.4 Can a business appoint a single Data Protection Officer to cover multiple entities?

The law and relevant rules do not specify whether a business can appoint a single Data Protection Officer to cover multiple entities.

7.5 Please describe any specific qualifications for the Data Protection Officer required by law.

Currently, there is no specific qualification for the Data Protection Officer required by law.

7.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?

Section 10.1 of the Standard provides that the Data Protection Officer’s responsibilities include but are not limited to:
1) comprehensive and overall implementation of the organisation’s personal data security and to be directly responsible for the personal data security;
2) drafting, issuing, implementing and regularly updating the privacy policy and related regulations;
3) establishing, maintaining, and updating the list of personal data held by the organisation (including the type, amount, origin, recipient, etc. of the personal data) and authorised access policies;
4) conducting a personal data security impact assessment;
5) organising a personal data security training;
6) conducting product or service testing before its release in case of unknown collection, use, sharing and other processing activities of personal data; and
7) conducting safety audits.

7.7 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?

Currently, the law does not require the appointment of a Data Protection Officer to be registered or notified to the relevant data protection authorities.

7.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?

Section 5.6 of the Standard provides the contents that the privacy policy should include, and the name of the Data Protection Officer is not within it. Nevertheless, there is the requirement to provide a person to contact for the public for the purpose of dealing with users’ queries and complaints regarding privacy and data protection issues.

8 Appointment of Processors

8.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?

The law does not have such requirements, but Article 8.1 of the Standard provides that a data controller may enter into an agreement with a trusted processor for it to process personal data on the controller’s behalf.
8.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?

There is no requirement for the formalities of the agreement. As for the content, Article 8.1 of the Standard stipulates that it should address the responsibilities and duties of the processor, including the requirements for processing the personal data, whether it can reassign a processor, the assistance it shall provide the data controller with, the responsibility to give feedback to the data controller and the responsibility in respect of terminating the agreement.

9 Marketing

9.1 Please describe any legislative restrictions on the sending of electronic direct marketing (e.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?).

Pursuant to Article 43 of the Advertisement Law, no organisation or individual shall, without obtaining the consent or request of the parties concerned, distribute advertisements to them via electronic means. Advertisements distributed via electronic means shall state the true identity and contact details of the senders, and the method for the recipients to refuse acceptance of future advertisements. Article 44 further provides that advertisements published in the form of pop-up windows on the website shall show the close sign prominently.

Article 13 of the Administration of Internet Electronic Mail Services Procedures provides that the word “advertisement” or “AD” must be indicated in the email subject, and it is prohibited to send emails containing commercial advertisement without the express consent of the receivers. Article 14 provides that if an email recipient who has expressly consented to receive electronic direct marketing subsequently refuses to continue receiving such emails, the sender shall stop sending such emails, unless otherwise agreed by the parties. The receivers shall be provided with the contact details for the discontinuation of the receipt of such electronic mails, including the email address of the sender, and shall ensure that such contact details are valid within 30 days.

Further, under Section 7.7 of the Standard, for advertising in electronic or other forms using personal data, the consent of relevant data subject must be obtained. If the data subject revokes his or her consent for data processing, the data controller shall not continue sending such advertisements.

9.2 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.).

Section VII of the Decision of the Standing Committee of the National People’s Congress on Strengthening Network Information Protection provides that any organisation or individual shall not send commercial electronic messages to the fixed-line, mobile telephone or e-mail box of an individual without the prior consent or request of the receivers or if the receivers explicitly express his/her rejection.

The operators of an e-commerce platform, when displaying search results of goods or services, shall mark “advertisement” for bid-ranked products or services, pursuant to Article 40 of the E-commerce Law. Furthermore, Article 18 provides that e-commerce business operators who provide search results based on consumers’ preference or consumption habits shall in the meantime provide options not targeting consumers’ personal characteristics.

9.3 Do the restrictions noted above apply to marketing sent from other jurisdictions?

The CSL, Advertisement Law and the E-commerce Law apply to operators providing products and services within the territory of the PRC, while for foreign operators providing products or services to the PRC on an offshore model, the law does not further elaborate whether it will apply or not. But according to Article 3.2 of the Draft Security Assessment Guidelines on Cross-Border Data Transfer, business operators not registered in China but providing products or services to China using the Chinese language, making settlement by the RMB, and delivering products to China are considered as “providing products or services to China”, in which case we understand that it is possible the relevant provisions will apply.

9.4 Is/are the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?

It appears that the data protection authorities are not particularly active, but there are recent cases where other authorities such as the Administration for Market Regulation are taking actions. For example, in 2017, Shanghai Paipaidai Finance Information Service Co., Ltd. was fined RMB800,000 for its infringement of the Advertisement Law, the breaches include, among others, sending direct advertisements via email without obtaining prior consent of the recipients.

9.5 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?

If the source of the marketing lists is legitimate and lawful and the data subject has consented, then it is not prohibited. Otherwise, it is illegal to do so, as network service providers and other enterprises, public institutions and their employees are obligated to keep strictly confidential a citizen’s personal electronic information collected during their business activities, and may not disclose, falsify, damage, sell or illegally provide such information to others, as provided in the Decision of the Standing Committee of the National People’s Congress on Strengthening Network Information Protection.

9.6 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?

Article 63 of the Advertisement Law provides that sending direct marketing communications without obtaining the consent of the target may result in a fine of up to RMB30,000.

E-commerce platforms not clearly mark “advertisement” for bid-ranked products may face a fine of up to RMB100,000, pursuant to Article 81 of the E-commerce Law and Article 59 of the Advertisement Law. In addition, Article 77 of the E-commerce Law provides that e-commerce business operators who provide search results in violation
10 Cookies

10.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).

There is no legislation addressing the use of cookies explicitly. Given that cookies fall within the definition of personal information (the CSL stipulates that personal data refers to information which can be used alone or in combination with other information to identify a natural person, the Standard also provides that information such as online browsing records is personal data), it is understood that the general regulations on personal data apply to the use of cookies.

10.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?

The law does not distinguish between different types of cookies at this stage.

10.3 To date, has/have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?

There are no administrative actions on the use of cookies. Nonetheless, in 2015, the search engine Baidu’s use of cookies to personalise advertisements aimed at consumers when they enter certain third-party websites was found by the court to be not infringing an individual’s right to privacy.

10.4 What are the maximum penalties for breaches of applicable cookie restrictions?

Please refer to the maximum penalties for other general breaches.

11 Restrictions on International Data Transfers

11.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.

The CSL provides that the personal information and important data collected by a CII operator during their operations within the territory of PRC shall be stored domestically, and the cross-border transfer of personal information and important data by a CII operator for business needs shall be subject to a security assessment. The Draft has expanded such obligation to all network operators. Furthermore, Article 11 of the Draft provides that the data shall not be transferred abroad in any of the following circumstances:

1) the personal data subject does not consent, or the outbound transmission of personal information jeopardises personal interests;
2) the outbound transmission imposes threats on the security of the nation’s politics, economy, technology and national defence, which may impose negative effects on national security and public interests; or
3) the CAC, public security department, security authority and other relevant authorities forbid such transmission.

The CAC and other relevant data protection authorities are in the process of updating the Draft; it remains uncertain whether the data localisation obligation will be expanded and imposed on all network operators.

11.2 Please describe the mechanisms businesses typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).

With the data subjects’ consent, companies can transfer data abroad, provided that such data does not satisfy any of the conditions listed under question 11.1 and a security assessment is properly carried out. In addition to obtaining the data subject’s consent, companies would need to prove that their transfer of personal data overseas arose from business needs, and would need to conduct a security assessment, according to the Draft. Under certain circumstances, they shall submit the assessment results to competent authorities for approval (see question 6.1).

11.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.

For CII operators, Article 37 of the CSL stipulates that personal data and important data collected or generated in China must be stored domestically. The transfer of such information overseas arising out of business needs is allowed, subject to the prior consent of the data subject, completion of a security assessment and approval from competent industry authorities.

For other network operators, Article 9 of the Draft stipulates that, where the data satisfy the conditions listed under question 6.1, the operator should notify the relevant authorities to conduct the security assessments.

12 Whistle-blower Hotlines

12.1 What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?

There is no rule explicitly addressing this matter.

12.2 Is anonymous reporting prohibited, strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do businesses typically address this issue?

Anonymous reporting is generally permitted.
13 CCTV

13.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?

Article 12 of the Public Security Video Image Information System Administrative Regulations (exposure draft, hereinafter the “CCTV Regulations”), which was issued by the Ministry of Public Security and regulates the use of CCTV for public safety purposes, stipulates that anyone who uses CCTV for public safety purposes shall notify the local public security department the type and location of the camera installed.

13.2 Are there limits on the purposes for which CCTV data may be used?

Pursuant to Article 6 of the CCTV Regulations, it is prohibited to obtain state secrets, work secrets, trade secrets from the public security video image information system, or infringe on citizens’ privacy by using such a system. The organisations that construct and use CCTV are required to keep in confidence the basic information (e.g., the system design, equipment type, installation location, address code) and collected data concerning state secrets, work secrets, trade secrets and shall not illegally disclose CCTV data concerning citizens’ privacy. Such CCTV data shall not be bought or sold, illegally used, copied or disseminated, pursuant to Article 22.

According to Article 21, investigative, procuratorial and judicial powers, public security and national security organs, as well as the administrative departments of the government at or above town level may inspect, copy or retrieve the basic information or data collected through CCTV.

In addition, under circumstances of security services, Article 25 of the Regulations on Administration of Security Services provides that the using of CCTV equipment shall not infringe on the legitimate rights and interests or privacy of individuals.

14 Employee Monitoring

14.1 What types of employee monitoring are permitted (if any), and in what circumstances?

On the one hand, Article 8 of the Labour Contract Law provides that employers are entitled to know about basic information of the worker in direct relation to the labour contract between them; therefore, some types of employee monitoring are permitted, though no specific rule explicitly addresses employee monitoring. On the other hand, it is prudent that the monitoring shall not infringe the employee’s privacy.

14.2 Is consent or notice required? Describe how employers typically obtain consent or provide notice.

Yes, the collecting of personal data generally requires consent from the data subject – this principle also applies to employee monitoring. In practice, such consent is normally obtained through a provision in the labour contract or in the employee handbook or similar documents.

14.3 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?

Article 4 of the Labour Contract Law requires employees to discuss with the employee representatives congress or all employees, and negotiate with trade union or employee representatives when formulating, revising or deciding on matters directly involving the vital interests of workers such as remuneration, working hours, rest periods and off days, labour safety and health, insurance and welfare, staff training, labour discipline and labour quota administration, etc. Article 43 further provides that employers shall notify the trade union when they unilaterally rescind a labour contract. But such notifying or negotiating circumstances may not directly relate to the employers’ monitoring or processing of employees’ personal data.

15 Data Security and Data Breach

15.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?

Under Article 40 of the CSL, network operators are responsible for taking technical and other necessary measures to ensure the security of personal data it collects, and to establish and improve the system for user information protection. But if the network operator as a controller appoints a third party to process personal data on its behalf, it shall ensure that such processor will provide an adequate level of protection to the personal data involved, as provided in Section 8.1 of the Standard.

15.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

Yes. Under Article 42 of the CSL, in case of (possible) disclosure, damage or loss of data collected, the network operator is required to take immediate remedies and report to the competent authority. Section 9.1 of the Standard provides that the report should include the type, quantity, content and nature of the affected data subjects, the impact of the breach, measures taken or to be taken, and the contact information of relevant persons.

15.3 Is there a legal requirement to report data breaches to affected data subjects? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

Yes. A network operator is required to take immediate remedies and notify the affected data subjects in case of (possible) data breaches pursuant to Article 42 of the CSL. Section 9.2 of the Standard stipulates that the content of the notification should include, but not be limited to, the nature and impact of the breach, the measures taken or to be taken, the suggestions for data subjects to mitigate risks, remedies for the data subjects and the contact information of the Data Protection Officer.
15.4 What are the maximum penalties for data security breaches?

Under Article 64 of the CSL, in case of severe violation, an operator or provider in breach of data security may face fines up to RMB1 million (or 10 times the illegal earnings), suspension of a related business, winding up for rectification, shutdown of any website/s and revocation of a business licence. The persons directly in charge may face a fine of up to RMB 100,000.

Data security breaches may also involve criminal liabilities. Article 286(A) of the Criminal Law stipulates that network service providers who do not fulfil legal obligations regarding information network security management, provided in the laws and administrative regulations, and refuse to make rectifications after being ordered by the relevant authorities (therefore causing the leakage of users’ information with serious consequences), may face a sentence of imprisonment or criminal detention of not more than three years or surveillance, with a fine or a fine only.

16 Enforcement and Sanctions

16.1 Describe the enforcement powers of the data protection authority(ies).

<table>
<thead>
<tr>
<th>Investigatory Power</th>
<th>Civil/Administrative Sanction</th>
<th>Criminal Sanction</th>
</tr>
</thead>
<tbody>
<tr>
<td>The public security departments have investigatory power regarding criminal and administrative infringement on personal data. The CAC, the telecommunications department, the public security department and other authorities concerned have investigatory power regarding administrative infringement on personal data.</td>
<td>The court is responsible for civil sanctions. The CAC, the telecommunications department, the public security department and other authorities concerned have the power to impose administrative sanctions.</td>
<td>The court has the power to impose criminal sanctions.</td>
</tr>
</tbody>
</table>

16.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?

Yes, and no court order is needed. For example, pursuant to Article 50 of the CSL, if any information prohibited by laws and administrative regulations from release or transmission is found, the CAC and other competent authorities may require the network operator to stop the transmission of such information, take measures such as deletion and keep the records. If any such information is from overseas, they may block the transmission.

16.3 Describe the data protection authority’s approach to exercising those powers, with examples of recent cases.

The CAC and relevant data protection authorities may issue a ban in the form of an administrative penalty, together with other punitive measures such as a fine, an order to rectify, etc. For relevant cases, please refer to question 18.1.

16.4 Does the data protection authority ever exercise its powers against businesses established in other jurisdictions? If so, how is this enforced?

So far, there is no public record of Chinese data protection authorities exercising their powers directly against companies established in other jurisdictions. In most cases, authorities may talk with the local subsidiary of an international company for its violations of CSL or other data protection regulations.

17 E-discovery / Disclosure to Foreign Law Enforcement Agencies

17.1 How do businesses typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?

In the case of foreign e-discovery requests from foreign law enforcement agencies, companies must obtain the consent of the personal data subject and do security assessments with the relevant authority before transmitting any personal data or important data abroad. However, in terms of security assessments, the Draft also provides that if there are different provisions under laws and regulations, such provisions shall apply, but in any event the consent of the personal data subject is required.

If there are treaties or agreements in relation to judicial assistance or cooperation entered into between China and the respective foreign country, the relevant companies may respond to such requests following such treaties or agreements. Furthermore, the International Criminal Judicial Assistance Law issued on Oct 26, 2018 set out rules and procedures regarding the enforcement of international criminal judicial assistance in China, including assistance requests of domestic agencies to foreign authorities, and foreign agencies’ requests of assistance in China. Pursuant to Article 4 of the International Criminal Judicial Assistance Law, businesses must obtain authorisation from relevant domestic agencies before disclosing any information or providing any assistance requested by foreign law enforcement agencies.

17.2 What guidance has/have the data protection authority(ies) issued?

The CAC have not issued any guidance particularly concerning e-discovery requests from foreign law enforcement agencies.

18 Trends and Developments

18.1 What enforcement trends have emerged during the previous 12 months? Describe any relevant case law.

The implementations of the CSL and other relevant legislations show that the Chinese legislators are gradually consummating the laws to protect national cyberspace sovereignty and network security. It is also a direct response to the harsh reality of personal data security currently in China. The enforcement authorities have kept a close eye on the illegal processing of personal data and have imposed administrative penalties on several internet companies.

In March 2018, the local branch of the People’s Bank of China (“PBOC”) imposed a fine of RMB180,000 on a well-known Chinese payment institution for its several illegal acts, including the
illegal processing of personal data. The payment institution was found to have been using personal financial information improperly and collecting personal financial information without following the principle of necessity.

In August 2018, a Chinese well-known social platform application was fined by a local Bureau of Administration for Market Regulation for its improper privacy settings in the application. The app users’ privacy setting interface were by default set to allow others to add them as friends, so that the subscriptions and preferences of the app users could be accessed by strangers. The penalty decision also states that the application failed to take technical measures and necessary methods to prevent the leakage of personal data.

In June 2018, the China Consumers Association (“CCA”) set out a project on evaluating and assessing the data collection activities and privacy policies of apps in China. In November 2018, CAC launched its assessment report on 100 apps, which points out several typical problems of the assessed apps, such as excessive collection of personal data, use of unclear privacy terms, etc.

18.2 What “hot topics” are currently a focus for the data protection regulator?

The illegal processing of personal data and privacy policies have been points of concern for the data protection regulators. In January 2019, the CAC, Ministry of Industry and Information Technology, MPC and SAMR jointly announced their “special campaign” against apps unlawfully collecting and using personal information. The authorities aim to intensify the supervision and punishment of unlawful collection and use of personal information and requires industrial associates to assess the privacy policies and the collection and use of personal information by apps that have a large user base and closely relate to people’s lives. Furthermore, in order to regulate the collection and use of user information by mobile apps, the CAC and SAMR launched the Implementation Rules on Security Certification for Mobile Internet Applications in March 2019 and encourage app operators to voluntarily pass app security certification.

In addition to CAC and SAMR’s actions, the public security authority issued its Guidelines of Personal Information Security Protection in Internet (the “Guidelines”) in April 2019, aiming to provide guidance for enterprises on personal information protection. The Guidelines require entities including cloud service providers to store personal information domestically, and provide rules for certain personal information processing scenarios such as precision marketing, targeted advertising, etc.
Susan Ning
King & Wood Mallesons
18th Floor, East Tower
World Financial Center
1 Dongsanhuan Zhonglu
Chaoyang District
Beijing 100020
P. R. China
Tel: +86 10 5878 5010
Email: susan.ning@cn.kwm.com
URL: www.kwm.com

Susan Ning is a senior partner and the head of the Commercial and Regulatory Group. She is one of the pioneers engaged in the cybersecurity and data compliance practice, with publications in a number of journals such as the Journal of Cyber Affairs. Her publications include New Trends of the US Personal Data Protection – Key Points of the New FCC Rules, Big Data: Success Comes Down to Solid Compliance, Does Your Data Need a "VISA" to Travel Abroad?, and A Brief Analysis on the Impact of Data on Competition in the Big Data Era, among others. Susan is recognised as a “Tier 1 Lawyer” for Cybersecurity and Data Compliance in 2019 LEGALBAND China. Susan’s practice areas cover self-assessment of network security, responding to network security checks initiated by authorities, data compliance training, due diligence of data transactions or exchanges, compliance of cross-border data transmissions, etc. Susan has assisted companies in sectors such as IT, transportation, online payment, consumer goods, finance, Internet of Vehicles in dealing with network security and data compliance issues.

Han Wu
King & Wood Mallesons
18th Floor, East Tower
World Financial Center
1 Dongsanhuan Zhonglu
Chaoyang District
Beijing 100020
P. R. China
Tel: +86 10 5878 5749
Email: wuhan@cn.kwm.com
URL: www.kwm.com

Han Wu practises in the areas of cybersecurity, data compliance and antitrust. He excels in providing cybersecurity and data compliance advice to multinational companies’ branches in China from the perspective of data compliance in China. Han also has expertise in establishing network security and data compliance systems for Chinese enterprises going abroad in line with the requirements of the European Union (GDPR), the United States and other cross-jurisdictions. Han was elected as one of “40-under-40 Data Lawyers” by Global Data Review in 2018.

In the area of cybersecurity and data compliance, Han provides legal services including: assisting clients to establish a cybersecurity compliance system; assisting clients in self-investigation on cybersecurity and data protection; assisting clients to conduct internal training on cybersecurity and data compliance; assisting clients in due diligence in data transactions; assisting clients to design plans for cross-border data transfers; and assisting clients in network security investigations and cybersecurity incidents, among others.
Chapter 13

Cyprus

Koushos Korfiotis Papacharalambous LLC

1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

Since 25 May 2018, the principal data protection legislation in the EU has been Regulation (EU) 2016/679 (the “General Data Protection Regulation” or “GDPR”). In Cyprus, a national law supplementing GDPR was enacted in July 2018, (L.125(I)/2018).

1.2 Is there any other general legislation that impacts data protection?

The following legislation impacts data protection in Cyprus:

- The Regulation of Electronic Communications and Postal Services Law of 2004, N.112(I)/2004 as amended to date, which implements the requirements of Directive 2002/58/EC (as amended by Directive 2009/136/EC) (the “ePrivacy Directive”), provides a specific set of privacy rules to harmonise the processing of personal data by the telecoms sector. In January 2017, the European Commission published a proposal for an ePrivacy Regulation (the “ePrivacy Regulation”) that would harmonise the applicable rules across the EU. In September 2018, the Council of the European Union published proposed revisions to the draft. The ePrivacy Regulation is still a draft at this stage and it is unclear when it will be finalised.

- Law N.28(III)/2001 implementing the Convention for the Protection of Individuals with regard to automatic processing of Personal Data and the Law N.30(III)/2003 implementing the Additional Protocol to the said Convention.

1.3 Is there any sector-specific legislation that impacts data protection?

The Prevention and Suppression of Money Laundering Activities Law (N.188(I)/2007), for example, imposes on the Compliance Officers of credit institutions the obligation to prepare and update lists categorising low- and high-risk clients with reference to their names, account numbers, etc.

1.4 What authority(ies) are responsible for data protection?

The Office of the Commissioner for Personal Data Protection (“the Commissioner”).

2 Definitions

2.1 Please provide the key definitions used in the relevant legislation:

- “Personal Data” means any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

- “Processing” means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

- “Controller” means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

- “Processor” means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

- “Data Subject” means an individual who is the subject of the relevant personal data.

- “Sensitive Personal Data” are the special categories of personal data, revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, data concerning health or sex life and sexual orientation, genetic data or biometric data.

- “Data Breach” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

3 Territorial Scope

3.1 Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to those laws?

The GDPR applies to businesses that are established in any EU
Member State, and that process personal data (either as a controller or processor, and regardless of whether or not the processing takes place in the EU) in the context of that establishment.

A business that is not established in any Member State, but is subject to the laws of a Member State by virtue of public international law, is also subject to the GDPR.

The GDPR applies to businesses outside the EU if they (either as controller or processor) process the personal data of EU residents in relation to: (i) the offering of goods or services (whether or not in return for payment) to EU residents; or (ii) the monitoring of the behaviour of EU residents (to the extent that such behaviour takes place in the EU).

Further, the GDPR applies to businesses established outside the EU if they monitor the behaviour of EU residents (to the extent such behaviour takes place in the EU).

### 4 Key Principles

#### 4.1 What are the key principles that apply to the processing of personal data?

- **Transparency**
  Personal data must be processed lawfully, fairly and in a transparent manner. Controllers must provide certain minimum information to data subjects regarding the collection and further processing of their personal data. Such information must be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

- **Lawful basis for processing**
  Processing of personal data is lawful only if, and to the extent that, it is permitted under EU data protection law. The GDPR provides an exhaustive list of legal bases on which personal data may be processed, of which the following are the most relevant for businesses: (i) prior, freely given, specific, informed and unambiguous consent of the data subject; (ii) contractual necessity (i.e., the processing is necessary for the performance of a contract to which the data subject is a party, or for the purposes of pre-contractual measures taken at the data subject’s request); (iii) compliance with legal obligations (i.e., the controller has a legal obligation, under the laws of the EU or an EU Member State, to perform the relevant processing); or (iv) legitimate interests (i.e., the processing is necessary for the purposes of legitimate interests pursued by the controller, except where the controller’s interest are overridden by the interests, fundamental rights or freedoms of the affected data subjects).

  Please note that businesses require stronger grounds to process special categories of personal data. The processing of special categories of personal data is only permitted under certain conditions, of which the most relevant for businesses are: (i) explicit consent of the affected data subject; (ii) the processing is necessary in the context of employment law; or (iii) the processing is necessary for the establishment, exercise or defence of legal claims.

- **Purpose limitation**
  Personal data may only be collected for specified, explicit and legitimate purposes and must not be further processed in a manner that is incompatible with those purposes. If a controller wishes to use the relevant personal data in a manner that is incompatible with the purposes for which they were initially collected, it must: (i) inform the data subject of such new processing; and (ii) must be able to rely on a lawful basis as set out above.

#### Data minimisation

Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which those data are processed. A business should only process the personal data that it actually needs to process in order to achieve its processing purposes.

- **Accuracy**
  Personal data must be accurate and, where necessary, kept up to date. A business must take every reasonable step to ensure that personal data that are inaccurate are either erased or rectified without delay.

- **Retention**
  Personal data must be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

- **Data security**
  Personal data must be processed in a manner that ensures appropriate security of those data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

- **Accountability**
  The controller is responsible for, and must be able to demonstrate, compliance with the data protection principles set out above.

### 5 Individual Rights

#### 5.1 What are the key rights that individuals have in relation to the processing of their personal data?

- **Right of access to data/copies of data**
  A data subject has the right to obtain from a controller the following information in respect of the data subject’s personal data: (i) confirmation of whether, and where, the controller is processing the data subject’s personal data; (ii) information about the purposes of the processing; (iii) information about the categories of data being processed; (iv) information about the categories of recipients with whom the data may be shared; (v) information about the period for which the data will be stored (or the criteria used to determine that period); (vi) information about the existence of the rights to erasure, to rectification, to restriction of processing and to object to processing; (vii) information about the existence of the right to complain to the relevant data protection authority; (viii) where the data were not collected from the data subject, information as to the source of the data; and (ix) information about the existence of, and an explanation of the logic involved in, any automated processing that has a significant effect on the data subject.

  Additionally, the data subject may request a copy of the personal data being processed.

- **Right to rectification of errors**
  Controllers must ensure that inaccurate or incomplete data are erased or rectified. Data subjects have the right to rectification of inaccurate personal data.

- **Right to deletion/right to be forgotten**
  Data subjects have the right to erasure of their personal data (the “right to be forgotten”) if: (i) the data are no longer needed for their original purpose (and no new lawful purpose exists); (ii) the lawful basis for the processing is the data subject’s consent, the data subject withdraws that consent, and no other lawful ground exists; (iii) the data subject exercises the right to...
Right to object to processing
Data subjects have the right to object, on grounds relating to their particular situation, to the processing of personal data where the basis for that processing is either public interest or legitimate interest of the controller. The controller must cease such processing unless it demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the relevant data subject or requires the data in order to establish, exercise or defend legal rights.

Right to restrict processing
Data subjects have the right to restrict the processing of personal data, which means that the data may only be held by the controller, and may only be used for limited purposes if: (i) the accuracy of the data is contested (and only for as long as it takes to verify that accuracy); (ii) the processing is unlawful and the data subject requests restriction (as opposed to exercising the right to erasure); (iii) the controller no longer needs the data for their original purpose, but the data are still required by the controller to establish, exercise or defend legal rights; or (iv) verification of overriding grounds is pending, in the context of an erasure request.

Right to data portability
Data subjects have a right to receive a copy of their personal data in a commonly used machine-readable format, and transfer their personal data from one controller to another or have the data transmitted directly between controllers.

Right to withdraw consent
A data subject has the right to withdraw their consent at any time. The withdrawal of consent does not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject must be informed of the right to withdraw consent. It must be as easy to withdraw consent as to give it.

Right to object to marketing
Data subjects have the right to object to the processing of personal data for the purpose of direct marketing, including profiling.

Right to complain to the relevant data protection authority(ies)
Data subjects have the right to lodge complaints concerning the processing of their personal data with the Commissioner, if the data subjects live in Cyprus or the alleged infringement occurred in Cyprus.

Right to basic information
Data subjects have the right to be provided with information on the identity of the controller, the reasons for processing their personal data, and other relevant information necessary to ensure the fair and transparent processing of personal data.

6 Registration Formalities and Prior Approval

6.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?
This is not applicable. Prior consultation is necessary in special circumstances: see question 10.3.

6.2 If such registration/notice is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?
See question 6.1.

6.3 On what basis are registrations/notifications made (e.g., per legal entity, per processing purpose, per data category, per system or database)?
See question 6.1.

6.4 Who must register with/notify the data protection authority (e.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation)?
See question 6.1.

6.5 What information must be included in the registration/notice (e.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes)?
See question 6.1.

6.6 What are the sanctions for failure to register/notify where required?
See question 6.1 and 15.1.

6.7 What is the fee per registration/notice (if applicable)?
See question 6.1.

6.8 How frequently must registrations/notices be renewed (if applicable)?
See question 6.1.

6.9 Is any prior approval required from the data protection regulator?
See question 6.1.

6.10 Can the registration/notice be completed online?
This is not applicable.

6.11 Is there a publicly available list of completed registrations/notices?
This is not applicable.
6.12 How long does a typical registration/notice process take?

This is not applicable.

### 7 Appointment of a Data Protection Officer

#### 7.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.

The appointment of a Data Protection Officer (DPO) for controllers or processors is only mandatory in some circumstances, in accordance with GDPR requirements, including where: (i) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity; (ii) there is large-scale regular and systematic monitoring of individuals; or (iii) there is large-scale processing of special categories of personal data.

Where a business designates a DPO voluntarily, the requirements of the GDPR apply as though the appointment were mandatory.

The Commissioner may establish and make public a list of processing operations and cases requiring the designation of a DPO, in addition to the cases referred to in Article 37 (1) of the GDPR.

#### 7.2 What are the sanctions for failing to appoint a Data Protection Officer where required?

In the circumstances where appointment of a DPO is mandatory, failure to comply may result in the wide range of penalties available under the GDPR.

#### 7.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect of his or her role as a Data Protection Officer?

The appointed DPO should not be dismissed or penalised for performing their tasks and should report directly to the highest management level of the controller or processor.

#### 7.4 Can a business appoint a single Data Protection Officer to cover multiple entities?

A single DPO is permitted by a group of undertakings provided that he or she is easily accessible from each establishment.

#### 7.5 Please describe any specific qualifications for the Data Protection Officer required by law.

The DPO should be appointed on the basis of professional qualities and should have an expert knowledge of data protection law and practices. While this is not strictly defined, it is clear that the level of expertise required will depend on the circumstances. For example, the involvement of large volumes of special categories of personal data will require a higher level of knowledge.

#### 7.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?

A DPO should be involved in all issues which relate to the protection of personal data. The GDPR outlines the minimum tasks required by the DPO which include: (i) informing the controller, processor and their relevant employees who process data of their obligations under the GDPR; (ii) monitoring compliance with the GDPR, national data protection legislation and internal policies in relation to the processing of personal data including internal audits; (iii) advising on data protection impact assessments and the training of staff; and (iv) co-operating with the data protection authority and acting as the authority’s primary contact point for issues related to data processing.

#### 7.7 Must the appointment of a Data Protection Officer be registered/ notified to the relevant data protection authority(ies)?

Yes. Also, under L.125(I)2018, the Commissioner may publish on the Office’s website a list of controllers and processors who have designated a DPO and their contact details, provided that the controller and the processor wish to be included in the list.

#### 7.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?

Not necessarily. However, the contact details of the DPO must be notified to the data subject when personal data relating to that data subject are collected. As a matter of good practice, the Article 29 Working Party (the “WP29”) (now the European Data Protection Board (the “EDPB”)) recommended in its 2017 guidance on DPOs that both the data protection authority and employees should be notified of the name and contact details of the DPO.

See also question 7.7.

### 8 Appointment of Processors

#### 8.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?

Yes. This agreement must set out the subject matter for processing, the duration of processing, the nature and purpose of processing, the types of personal data and categories of data subjects and the obligations and rights of the controller (i.e., the business). Specifically, the agreement must include all the required information under GDPR Article 28(3).

#### 8.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?

The processor must be appointed under a binding agreement in writing. The contractual terms must stipulate that the processor: (i) only acts on the documented instructions of the controller; (ii) imposes confidentiality obligations on all employees; (iii) ensures the security of personal data that it processes; (iv) abides by the rules of regarding the appointment of sub-processors; (v) implements
measures to assist the controller with guaranteeing the rights of data subjects; (vi) assists the controller in obtaining approval from the relevant data protection authority; (vii) either returns or destroys the personal data at the end of the relationship (except as required by EU or Member State law); and (viii) provides the controller with all information necessary to demonstrate compliance with the GDPR.

9 Marketing

9.1 Please describe any legislative restrictions on the sending of electronic direct marketing (e.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?).

Marketing communications are covered by Article 106 of the Regulation of Electronic Communications and Post Law N.112(I)/2004. The prior free and informed consent of the data subject is required, except where the data subject is an existing customer of the data controller and the marketing communications relate to the promotion of goods or services similar to those already received from the data subject by the data controller, in which case direct marketing is allowed provided the data subject is given the opportunity to opt out, free of charge and easily.

9.2 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.).

See question 9.1

9.3 Do the restrictions noted above apply to marketing sent from other jurisdictions?

This is not applicable.

9.4 Is/are the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?

Yes. The Commissioner has, since 2005, dealt with 11 cases of marketing restrictions violations. The fines imposed vary within the range of €400–€8,000 by mitigating and aggravating factors, such as whether the violation was a one-off incident or repetitive, whether the perpetrator immediately admitted to a breach, whether the number of complainants was small or large, and whether measures to avoid future breach of the law were taken or not and if this influenced the Commissioner’s decision on the sanction to be imposed.

The most recent administrative penalty, of €1,000 for a violation of section 106 of Law 112(I)/2004, was imposed by the Commissioner against a pizza shop due to the sending of a message without allowing the addressee to stop receives the messages in an easy way.

9.5 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?

This issue has been dealt with by the Commissioner, who has issued fines against unlawful data processing for marketing purposes by various candidates during political elections. The Commissioner has issued the following guidance: “[C]andidates should provide a list of the recipients’ numbers or addresses. If advertisers maintain their own list, they must be able to ensure that they have received the consent of the recipients with regard to the particular type of advertising requested by the candidate (e.g. the recipients have stated that they are interested in receiving political messages from anyone). In messages sent, it should be clear who the advertiser is who has sent the messages on behalf of the candidate. The above details must be provided in a contract between the candidate and the advertising company, which has the status of data processor.”

9.6 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?

The Law 112(I)/2004 (which implements Directive 2002/58/EC) refers to the power of the Data Protection Commissioner to impose fines in accordance with the Cyprus Data Protection Law. Therefore, the Commissioner is entitled to impose penalties within the maximum level provided in the GDPR and in accordance with the relevant provisions of L.125(I)2018.

10 Cookies

10.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).

Law N.112(I)/2004, with its amendment in 2012, implements Article 5 of the ePrivacy Directive (2009/136/EC). Pursuant to Article 5 of the EU ePrivacy Directive, the storage of cookies (or other data) on an end user’s device requires prior consent (the applicable standard of consent is derived from the GDPR). This does not apply if: (i) the cookie is for the sole purpose of carrying out the transmission of a communication over an electronic communications network; or (ii) the cookie is strictly necessary to provide an “information society service” (e.g., a service over the internet) requested by the subscriber or user, which means that it must be essential to fulfill their request.

The EU Commission intends to pass a new ePrivacy Regulation that will replace the respective national legislation in the EU Member States. The ePrivacy Regulation is planned to come into force in 2019.

10.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?

See question 9.7.

10.3 To date, has/have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?

No, there has been no enforcement action.

10.4 What are the maximum penalties for breaches of applicable cookie restrictions?

See question 9.6.
**11 Restrictions on International Data Transfers**

**11.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.**

Data transfers to other jurisdictions that are not within the European Economic Area (the “EEA”) can only take place if the transfer is to an “Adequate Jurisdiction” (as specified by the EU Commission), the business has implemented one of the required safeguards as specified by the GDPR, or one of the derogations specified in the GDPR applies to the relevant transfer. The EDPB Guidelines (2/2018) set out that a “layered approach” should be taken with respect to these transfer mechanisms. If the transfer is not to an Adequate Jurisdiction, the data exporter should first explore the possibility of implementing one of the safeguards provided for in the GDPR before relying on a derogation.

For restrictions on transfers of special categories of data, see question 10.3.

**11.2 Please describe the mechanisms businesses typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).**

In the absence of an Adequate Jurisdiction, the GDPR offers a number of ways to ensure compliance for international data transfers, of which one is consent of the relevant data subject. Other common options are the use of Standard Contractual Clauses or BCReS.

Businesses can adopt the Standard Contractual Clauses drafted by the EU Commission – these are available for transfers between controllers, and transfers between a controller (as exporter) and a processor (as importer). International data transfers may also take place on the basis of contracts agreed between the data exporter and data importer provided that they conform to the protections outlined in the GDPR, and they have prior approval by the relevant data protection authority.

International data transfers within a group of businesses can be safeguarded by the implementation of Binding Corporate Rules (“BCRs”). The BCRs need approval from the relevant data protection authority and must specify the information required under Article 49 GDPR.

Transfer of personal data to the USA is also possible if the data importer has signed up to the EU-US Privacy Shield Framework, which was designed by the US Department of Commerce and the EU Commission to provide businesses in the EU and the US with a mechanism to comply with data protection requirements when transferring personal data from the EU to the US.

**11.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.**

L.125(I) 2018 PART VII provides that when the controller or the processor intends to transfer special categories of personal data to a third country or to an international organisation on the basis of the appropriate safeguards provided for in Article 46, or on the basis of the BCR provided for in Article 47 of the GDPR, the Commissioner must be informed of their intention before transferring such data. Also, a transfer carried out by a controller or processor, of special categories of personal data to a third country or an international organisation, which is based on derogations for specific situations provided for in Article 49 of the GDPR, requires an impact assessment to be undertaken, as well as prior consultation with the Commissioner.

**12 Whistle-blower Hotlines**

**12.1 What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?**

Internal whistle-blowing schemes are generally established in pursuance of a concern to implement proper corporate governance principles in the daily functioning of businesses. Whistle-blowing is designed as an additional mechanism for employees to report misconduct internally through a specific channel and supplements a business’ regular information and reporting channels, such as employee representatives, line management, quality-control personnel or internal auditors who are employed precisely to report such misconduct.

The WP29 has limited its Opinion 1/2006 on the application of EU data protection rules to internal whistle-blowing schemes to the fields of accounting, internal accounting controls, auditing matters, the fight against bribery, banking and financial crime. The scope of corporate whistle-blower hotlines, however, does not need to be limited to any particular issues. In the Opinion it is recommended that the business responsible for the whistle-blowing scheme should carefully assess whether it might be appropriate to limit the number of persons eligible for reporting alleged misconduct through the whistle-blowing scheme, and whether it might be appropriate to limit the number of persons who may be reported through the scheme, in particular in the light of the seriousness of the alleged offences reported.

**12.2 Is anonymous reporting prohibited, strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do businesses typically address this issue?**

Anonymous reporting is not prohibited under EU data protection law; however, it raises problems as regards the essential requirement that personal data should only be collected fairly. In Opinion 1/2006, the WP29 considered that only identified reports should be advertised in order to satisfy this requirement. Businesses should not encourage or advertise the fact that anonymous reports may be made through a whistle-blower scheme.

An individual who intends to report to a whistle-blowing system should be aware that he/she will not suffer due to his/her action. The whistle-blower, at the time of establishing the first contact with the scheme, should be informed that his/her identity will be kept confidential at all the stages of the process, and in particular will not be disclosed to third parties, such as the incriminated person or to the employee’s line management. If, despite this information, the person reporting to the scheme still wants to remain anonymous, the report will be accepted into the scheme. Whistle-blowers should be informed that their identity may need to be disclosed to the relevant people involved in any further investigation or subsequent judicial proceedings instigated as a result of any enquiry conducted by the whistle-blowing scheme.
The Commissioner advises controllers to avoid anonymous reporting, or to have internal procedures for handling such reporting.

13 CCTV

13.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?

No. However, the Commissioner has issued specific Guidance on the use of CCTV and has recently emphasised the necessity for organisations and businesses to conduct a data protection impact assessment (“DPIA”) in accordance with Article 35 of the GDPR.

13.2 Are there limits on the purposes for which CCTV data may be used?

Based on a recent decision from the Commissioner, “the recording of audio (conversations) data through the CCTV system is considered to be highly intrusive to individuals’ privacy, infringes human dignity and is generally banned in all cases”.

14 Employee Monitoring

14.1 What types of employee monitoring are permitted (if any), and in what circumstances?

The employer must be able to justify the legality and necessity of control and monitoring, and that there is no other less intrusive method for carrying out the objectives pursued. The legitimate interest invoked by the employer, in order to be justified, must prevail over the rights, interests and fundamental freedoms of employees.

14.2 Is consent or notice required? Describe how employers typically obtain consent or provide notice.

Employers must in all cases inform the employees about the purpose, manner and duration of control and monitoring they intend to apply prior to the beginning of the monitoring. It is good practice for the employer to adopt a written policy for determining the parameters of telephone use, computer, internet, other electronic means of communication and material/equipment of the company/organisation of employees, and ways/systems with which the employer will monitor/control its use. Secret surveillance or monitoring of employees is never permitted, as employees must be notified in advance.

Directives from the Commissioner suggest avoiding consent as a legal basis for processing employees’ data, due to the imbalance of power between the employer and the employees, which might render the consent in question as not freely given or unambiguous.

14.3 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?

According to the Commissioner’s guidelines, it is good practice for employers to consult employee representatives and trade unions prior to the installation and use of control measures within the workplace.

15 Data Security and Data Breach

15.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?

Yes. Personal data must be processed in a way which ensures security and safeguards against unauthorised or unlawful processing, accidental loss, destruction and damage of the data.

Both controllers and processors must ensure they have appropriate technical and organisational measures to meet the requirements of the GDPR. Depending on the security risk, this may include: the encryption of personal data; the ability to ensure the ongoing confidentiality, integrity and resilience of processing systems; an ability to restore access to data following a technical or physical incident; and a process for regularly testing and evaluating the technical and organisational measures taken to ensure the security of processing.

15.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

The controller is responsible for reporting a personal data breach without undue delay (and in any case within 72 hours of first becoming aware of the breach) to the Commissioner, unless the breach is unlikely to result in a risk to the rights and freedoms of the data subject(s). A processor must notify any data breach to the controller without undue delay.

The notification must include the nature of the personal data breach including: the categories and number of data subjects concerned; the name and contact details of the DPO or relevant point of contact; the likely consequences of the breach; and the measures taken to address the breach, including attempts to mitigate possible adverse effects.

15.3 Is there a legal requirement to report data breaches to affected data subjects? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

Controllers have a legal requirement to communicate the breach to the data subject, without undue delay, if the breach is likely to result in a high risk to the rights and freedoms of the data subject.

The notification must include the name and contact details of the DPO (or point of contact), the likely consequences of the breach, and any measures taken to remedy or mitigate the breach.

The controller may be exempt from notifying the data subject if the risk of harm is remote (e.g., because the affected data is encrypted), the controller has taken measures to minimise the risk of harm (e.g., suspending affected accounts), or the notification requires a disproportionate effort (e.g., a public notice of the breach).

15.4 What are the maximum penalties for data security breaches?

The maximum penalty is the higher of €20 million or 4% of worldwide turnover.
### 16 Enforcement and Sanctions

#### 16.1 Describe the enforcement powers of the data protection authority(ies).

<table>
<thead>
<tr>
<th>Investigatory Power</th>
<th>Civil/Administrative Sanction</th>
<th>Criminal Sanction</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Investigatory Powers</strong></td>
<td>The Commissioner:</td>
<td>The Commissioner shall notify to the AG of the Republic and/or to the police any contravention of the provisions of the GDPR or of the L.125(I)2018, that may constitute an offence in accordance with Section 33 of L.125(I)2018 provisions below.</td>
</tr>
<tr>
<td>■ may not investigate a complaint or discontinue its investigation for reasons of public interest and shall notify the data subject, within a reasonable period, of the reasons for doing so.</td>
<td>■ a controller or a processor who does not maintain the record of processing activities as per Article 30 of the GDPR or provides false, inaccurate, incomplete or misleading information to the Commissioner in relation to this record;</td>
<td></td>
</tr>
<tr>
<td>■ shall have access to all the personal data and to all the information required for the performance of his or her tasks and the exercise of his or her powers, including confidential information, except for information covered by legal professional privilege;</td>
<td>■ a controller or a processor who does not cooperate with the Commissioner in the performance of its tasks;</td>
<td></td>
</tr>
<tr>
<td>■ shall have the power to enter, without necessarily informing the controller or the processor or their representative in advance, in any office, professional premises or means of transport, with the exception of residences; and</td>
<td>■ a controller who does not notify to the Commissioner a personal data breach, in accordance with the provisions of Article 33 (1) of the GDPR; or, in the case of a processor, in accordance with the provisions Article 33 (2), paragraph 2 of the GDPR;</td>
<td></td>
</tr>
<tr>
<td>■ for the exercise of the investigative powers the Commissioner, may:</td>
<td>■ for the exercise of the investigative powers the Commissioner, may:</td>
<td></td>
</tr>
<tr>
<td>■ be assisted by an expert and/or the police; and</td>
<td>■ seize documents or electronic equipment by virtue of a search warrant in accordance with the Criminal Procedure Law.</td>
<td></td>
</tr>
<tr>
<td>■ seize documents or electronic equipment by virtue of a search warrant in accordance with the Criminal Procedure Law.</td>
<td>■ a controller who does not communicate a personal data breach to the data subject, in accordance with Article 34 of the GDPR;</td>
<td></td>
</tr>
<tr>
<td><strong>Corrective Powers</strong></td>
<td>The Commissioner shall require the Cyprus Organization for the Promotion of Quality to revoke the accreditation of a certification body, when the Commissioner ascertains that the requirements for the certification are not or are no longer met or where actions taken by the certification body violate the provisions of the Regulation or of L.125(I)2018.</td>
<td>■ a controller who does not carry out an impact assessment, in breach of Article 35 (1) of the GDPR or of L.125(I)2018;</td>
</tr>
<tr>
<td>■ The Commissioner shall denounce the Cyprus Organization for the Promotion of Quality to the European Commission, in the event the organisation does not revoke an accreditation of a certification body in accordance with L.125(I)2018.</td>
<td>■ a controller or a processor who prevents the DPO from performing his or her tasks;*</td>
<td></td>
</tr>
<tr>
<td>■ The Commissioner shall inform, where appropriate, the data subject, the controller and the processor of the time limits provided for in Articles 60 to 66 of the GDPR.</td>
<td>■ a certification body which issues or does not withdraw a certification, in accordance with the provisions of Article 42 of the GDPR;</td>
<td></td>
</tr>
<tr>
<td>■ The Commissioner may establish and make public the list of processing operations and cases that require the designation of a DPO.</td>
<td>■ a controller or a processor who transfers personal data to a third country or an international organisation, in breach of Chapter V of the GDPR;</td>
<td></td>
</tr>
<tr>
<td>■ In addition to the authorisation and advisory powers provided for in the GDPR, the Commissioner shall have the power to:</td>
<td>■ a controller or a processor who transfers personal data to a third country or an international organisation, in breach of the explicit limits imposed by the Commissioner in accordance with L.125(I)2018;*</td>
<td></td>
</tr>
<tr>
<td>■ authorise the combination of filing systems in accordance with L.125(I)2018 and impose terms and conditions for the materialisation of the combination;</td>
<td>■ a person who intervenes without the right, in any way, in a filing system or acquires knowledge of the personal data thereof or removes, alters, damages, destroys, processes or uses in any way, discloses, communicates, renders them accessible to non-authorised persons or allows these persons to acquire knowledge of the said data, for gainful purposes or not; or</td>
<td></td>
</tr>
<tr>
<td>■ impose terms and conditions in relation to the application of the measures for the restriction of the rights referred to in section 11 of this Law;</td>
<td>■ a controller or processor who prevents or impairs the exercise of the Commissioner’s powers.</td>
<td></td>
</tr>
<tr>
<td>■ impose terms and conditions for the exemption to the obligation to communicate the data breach;</td>
<td>* If a person is convicted of committing this offence, which damages the interests of the Republic or impairs the free governing of the Republic or compromises national security, he or she shall be subject to imprisonment which shall not exceed five (5) years, or to a fine which shall not exceed 50,000 euros, or to both of these penalties.</td>
<td></td>
</tr>
<tr>
<td>■ impose explicit limits for the transfer of special categories of personal data;</td>
<td>2. If a person is convicted for committing any of the following offences, he or she shall be subject to imprisonment which shall not exceed one (1) year, or to a fine which shall not exceed 10,000 euros or to both of these penalties:</td>
<td></td>
</tr>
<tr>
<td>(Continued overleaf.)</td>
<td>(Continued overleaf.)</td>
<td></td>
</tr>
</tbody>
</table>
16.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?

This is not applicable.

16.3 Describe the data protection authority’s approach to exercising those powers, with examples of recent cases.

The Commissioner’s Office has provided organisations and businesses with sufficient information and presentations regarding the necessary steps for compliance, prior to May 2018 (GDPR enforcement date). Since then, the Commissioner’s Office has identified the following as the main areas of non-compliance, either by responding to complaints or on its own initiative:

- Failure to keep and maintain a Record of Processing Activities as per Article 30 of the GDPR.
- Failure and gaps of the organisations in providing sufficient information to their DPOs in order to perform their tasks.
- Lack of procedures to implement proper technical and organisational measures, or apply easy and free ways of unsubscribing from direct marketing communications.

A few of the recent cases include the following:

1. Administrative fine of €5,000 against a hospital for loss of a patient’s file.
2. Administrative fine of €10,000 against a newspaper for the unlawful disclosure of names and photographs of police investigators.
3. Administrative fine of €500 against a university for sending SMS messages to a student without providing the ability to stop receiving messages free of charge.

16.4 Does the data protection authority ever exercise its powers against businesses established in other jurisdictions? If so, how is this enforced?

This is not applicable.
18.2 What “hot topics” are currently a focus for the data protection regulator?

With the emergence of highly advanced technologies and the EU’s pledge of creating a digital single market, the Commissioner’s Office is monitoring the trends and technological advances such as blockchain, artificial intelligence, the Internet of Things, and other innovative profiling methods. The Commissioner’s Office is aware of the potential privacy implications arising from the use of such technologies and is continuously observing the EU relevant legislation and guidance for more updates.

Loizos Papacharalambous
Koushos Korfiotis Papacharalambous LLC
20 Costi Palama str.
Aspelia Court
1096 Nicosia
Cyprus

Tel: +357 22 664 555
Email: loizosp@kkplaw.com
URL: www.kkplaw.com

Loizos has been a member of the Cyprus Bar Association since 2004. He graduated from the University of Bristol before going on to successfully complete the Bar Vocational Course, becoming a member of Gray’s Inn. In 2006, Loizos successfully completed the International and Comparative Commercial Arbitration Diploma with Queen Mary College of the University of London. In 2011, Loizos was admitted as a Member of The Chartered Institute of Arbitrators. Loizos is currently attending courses to obtain an M.Sc. in Finance and Banking. His main areas of practice are commercial and corporate litigation and representation of banks, investment and insurance companies.

Loizos has been the Vice-Chairman of the Cyprus Telecommunications Authority (CYTA), the Vice-President of the Nicosia Bar Association and the Chairman of the Housing Finance Corporation.

Anastasios Kareklas
Koushos Korfiotis Papacharalambous LLC
20 Costi Palama str.
Aspelia Court
1096 Nicosia
Cyprus

Tel: +357 22 664 555
Email: akareklas@kkplaw.com
URL: www.kkplaw.com

Anastasios is a lawyer at Koushos Korfiotis Papacharalambous LLC, with wide-ranging knowledge and experience on IT legal matters, with a particular focus on Data Protection Law and e-Commerce Law. Anastasios holds an LL.B. (Hons) from the University of Sussex and an LL.M. in Computer and Communications Law from Queen Mary University of London (QMUL). Anastasios is a Certified Information Privacy Professional (CIPP/E) by the International Association of Privacy Professionals (IAPP), acts as Data Protection Officer and is a key member of the Data Protection Team at KKP LLC. He provides consultation on compliance issues and legal advice on data protection for clients.
Chapter 14

Denmark

Integra Law Firm

Sissel Kristensen
Heidi Højmark Helveg

1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

Since 25 May 2018, the principal data protection legislation in the EU has been Regulation (EU) 2016/679 (the “General Data Protection Regulation” or “GDPR”). The GDPR repealed Directive 95/46/EC (the “Data Protection Directive”) and has led to increased (though not total) harmonisation of data protection law across the EU Member States.

1.2 Is there any other general legislation that impacts data protection?

On 23 May 2018, the act on supplementary provisions to the regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (the “Data Protection Act” or the “DP Act”) was adopted and enforced. Executive Order of 14 December 2011 (the “Cookie Order”) implements the ePrivacy Directive 2002/58/EC (as amended by Directive 2009/136/EC) (the “ePrivacy Directive”), which provides a specific set of privacy rules to harmonise the processing of personal data by the telecoms sector. In January 2017, the European Commission published a proposal for an ePrivacy regulation (the “ePrivacy Regulation”) that would harmonise the applicable rules across the EU. In September 2018, the Council of the European Union published proposed revisions to the draft. The ePrivacy Regulation is still a draft at this stage and it is unclear when it will be finalised.

Act no. 128 on Electronic Communications Networks and Services of 7 February 2014 (the “Tele Act”) Executive Order on the retention and storage of traffic data by providers of electronic communications networks and services, No. 988 of 28 September 2006, as amended by executive order of amendment no. 660 of 19 June 2014 (the “Retention Order”) implements parts of the Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.

1.3 Is there any sector-specific legislation that impacts data protection?

Yes, there is sector-specific data protection regulation in the following sectors:
- the telecommunications sector;
- the financial sector; and
- the criminal enforcement field.

1.4 What authority(ies) are responsible for data protection?

Principally, the Danish Data Protection Agency (the “DPA”) is the supervisory authority with responsibility for compliance with the GDPR and the DP Act. The Danish Court Administration supervises the processing of data carried out for the courts when they do not act in their capacity of courts. The Danish Business Authority is the supervisory authority for the regulation on cookies and telecommunication.

2 Definitions

2.1 Please provide the key definitions used in the relevant legislation:

- “Personal Data” means any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
- “Processing” means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
- “Controller” means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
- “Processor” means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
- “Data Subject” means an individual who is the subject of the relevant personal data.
Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to those laws?

The GDPR applies to businesses that are established in any EU Member State, and that process personal data (either as a controller or processor, and regardless of whether the processing takes place in the EU) in the context of that establishment.

A business that is not established in any Member State but is subject to the laws of a Member State by virtue of public international law is also subject to the GDPR.

The GDPR applies to businesses outside the EU if they (either as controller or processor) process the personal data of EU residents in relation to: (i) the offering of goods or services (whether or not in return for payment) to EU residents; or (ii) the monitoring of the behaviour of EU residents (to the extent that such behaviour takes place in the EU).

Further, the GDPR applies to businesses established outside the EU if they monitor the behaviour of EU residents (to the extent such behaviour takes place in the EU).

What are the key principles that apply to the processing of personal data?

Transparency

Personal data must be processed lawfully, fairly and in a transparent manner. Controllers must provide certain minimum information to data subjects regarding the collection and further processing of their personal data. Such information must be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

Lawful basis for processing

Processing of personal data is lawful only if, and to the extent that, it is permitted under EU data protection law. The GDPR provides an exhaustive list of legal bases on which personal data may be processed, of which the following are the most relevant for businesses: (i) prior, freely given, specific, informed and unambiguous consent of the data subject; (ii) contractual necessity (i.e., the processing is necessary for the performance of a contract to which the data subject is a party, or for the purposes of pre-contractual measures taken at the data subject’s request); (iii) compliance with legal obligations (i.e., the controller has a legal obligation, under the laws of the EU or an EU Member State, to perform the relevant processing); or (iv) legitimate interests (i.e., the processing is necessary for the purposes of legitimate interests pursued by the controller, except where the controller’s interests are overridden by the interests, fundamental rights or freedoms of the affected data subjects).

Please note that businesses require stronger grounds to process sensitive personal data. The processing of sensitive personal data is only permitted under certain conditions, of which the most relevant for businesses are: (i) explicit consent of the affected data subject; (ii) the processing is necessary in the context of employment law; or (iii) the processing is necessary for the establishment, exercise or defence of legal claims.

Purpose limitation

Personal data may only be collected for specified, explicit and legitimate purposes and must not be further processed in a manner that is incompatible with those purposes. If a controller wishes to use the relevant personal data in a manner that is incompatible with the purposes for which they were initially collected, it must: (i) inform the data subject of such new processing; and (ii) must be able to rely on a lawful basis as set out above.

Data minimisation

Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which those data are processed. A business should only process the personal data that it actually needs to process in order to achieve its processing purposes.

Accuracy

Personal data must be accurate and, where necessary, kept up to date. A business must take every reasonable step to ensure that personal data that are inaccurate are either erased or rectified without delay.

Retention

Personal data must be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

Data security

Personal data must be processed in a manner that ensures appropriate security of those data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Accountability

The controller is responsible for, and must be able to demonstrate, compliance with the data protection principles set out above.
Additionally, the data subject may request a copy of the personal data being processed.

- **Right to rectification of errors**
Controllers must ensure that inaccurate or incomplete data are erased or rectified. Data subjects have the right to rectification of inaccurate personal data.

- **Right to deletion/right to be forgotten**
Data subjects have the right to erasure of their personal data (the “right to be forgotten”) if: (i) the data are no longer needed for their original purpose (and no new lawful purpose exists); (ii) the lawful basis for the processing is the data subject’s consent, the data subject withdraws that consent, and no other lawful ground exists; (iii) the data subject exercises the right to object, and the controller has no overriding grounds for continuing the processing; (iv) the data have been processed unlawfully; or (v) erasure is necessary for compliance with EU law or national data protection law.

- **Right to object to processing**
Data subjects have the right to object, on grounds relating to their particular situation, to the processing of personal data where the basis for that processing is either public interest or the legitimate interest of the controller. The controller must cease such processing unless it demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the relevant data subject or requires the data in order to establish, exercise or defend legal rights.

- **Right to restrict processing**
Data subjects have the right to restrict the processing of personal data, which means that the data may only be held by the controller, and may only be used for limited purposes if: (i) the accuracy of the data is contested (and only for as long as it takes to verify that accuracy); (ii) the processing is unlawful and the data subject requests restriction (as opposed to exercising the right to erasure); (iii) the controller no longer needs the data for their original purpose, but the data are still required by the controller to establish, exercise or defend legal rights; or (iv) verification of overriding grounds is pending, in the context of an erasure request.

- **Right to data portability**
Data subjects have a right to receive a copy of their personal data in a commonly used machine-readable format and transfer their personal data from one controller to another or have the data transmitted directly between controllers.

- **Right to withdraw consent**
A data subject has the right to withdraw their consent at any time. The withdrawal of consent does not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject must be informed of the right to withdraw consent. It must be as easy to withdraw consent as to give it.

- **Right to object to marketing**
Data subjects have the right to object to the processing of personal data for the purpose of direct marketing, including profiling.

- **Right to complain to the relevant data protection authority(ies)**
Data subjects have the right to lodge complaints concerning the processing of their personal data with the Danish Data Protection Agency, if the data subjects live in Denmark or the alleged infringement occurred in Denmark.

- **Right to basic information**
Data subjects have the right to be provided with information on the identity of the controller, the reasons for processing their personal data and other relevant information necessary to ensure the fair and transparent processing of personal data.

### 6 Registration Formalities and Prior Approval

#### 6.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?

According to the DP Act, private data controllers shall obtain an authorisation from the DPA prior to the processing of personal data where the processing of data is carried out (i) for the purpose of warning others against having business relations or accepting employment with a certain data subject, (ii) for the purpose of commercial disclosure of data for the assessment of financial standing and creditworthiness, or (iii) exclusively for the purpose of operating legal information systems. Amendments also require authorisation. The DPA will lay down terms for the processing.

The processing of data covered by Article 9(1) of the GDPR may take place if the processing is necessary for reasons of substantial public interest, cf. point g) of Article 9(2) of GDPR. Private data controllers shall obtain an authorisation from the DPA prior to such processing of personal data. The DPA will lay down terms for the processing.

According to the Danish Act on information databases operated by the mass media, mass media shall notify the DPA of editorial information databases and publicly available information databases.

#### 6.2 If such registration/ notification is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?

The controller shall provide the DPA with specific information on the processing e.g. “listing all processing activities, categories of data”, cf. question 6.5.

#### 6.3 On what basis are registrations/notifications made (e.g., per legal entity, per processing purpose, per data category, per system or database)?

Registrations and notifications are made according to the processing purpose.

#### 6.4 Who must register with/notify the data protection authority (e.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation)?

In very few cases, private controllers have an obligation to notify the DPA and obtain approval prior to processing personal data for specific purposes.

#### 6.5 What information must be included in the registration/notification (e.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes)?

An authorisation application requires information on:

- name and contact details of the controller (including any joint controller, representative and data protection officer);
7 Appointment of a Data Protection Officer

7.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.

The appointment of a Data Protection Officer for controllers or processors is only mandatory in some circumstances, including where there is: (i) large-scale regular and systematic monitoring of individuals; or (ii) large-scale processing of sensitive personal data. Also, all public authorities must appoint a Data Protection Officer. Where a business designates a Data Protection Officer voluntarily, the requirements of the GDPR apply as though the appointment were mandatory.

7.2 What are the sanctions for failing to appoint a Data Protection Officer where required?

In the circumstances where appointment of a Data Protection Officer is mandatory, failure to comply may result in the wide range of penalties available under the GDPR.

7.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect of his or her role as a Data Protection Officer?

Yes, and hence the appointed Data Protection Officer should not be dismissed or penalised for performing tasks and should report directly to the highest management level of the controller or processor.

7.4 Can a business appoint a single Data Protection Officer to cover multiple entities?

A single Data Protection Officer may be appointed by a group of undertakings provided that the Data Protection Officer is easily accessible from each establishment.

7.5 Please describe any specific qualifications for the Data Protection Officer required by law.

The Data Protection Officer should be appointed on the basis of professional qualities and should have an expert knowledge of data protection law and practices. While this is not strictly defined, it is clear that the level of expertise required will depend on the specific circumstances. For example, the involvement of large volumes of sensitive personal data will require a higher level of knowledge than that of smaller volumes.

7.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?

A Data Protection Officer should be involved in all issues which relate to the protection of personal data. The GDPR outlines the minimum tasks required by the Data Protection Officer, which include: (i) informing the controller, processor and their relevant employees who process data of their obligations under the GDPR; (ii) monitoring compliance with the GDPR, national data protection legislation and internal policies in relation to the processing of personal data including internal audits; (iii) advising on data protection impact.

6.6 What are the sanctions for failure to register/notify where required?

The provisions on notification of the DPA are based on Article 36, subsection 5 of the GDPR, and the sanctions for non-compliance with the obligation to obtain an authorisation follow the sanction for non-compliance with Article 36, subsection 5. The purpose of the mass media notification is to exclude the mass media information databases from the scope of the GDPR and DP Act. There are no sanctions for mass media’s failure to notify the DPA of the information databases. If a mass media organisation fails to notify the DPA, the media’s processing of personal data in the information database will be subject to the DP Act and the GDPR.

6.7 What is the fee per registration/notification (if applicable)?

There is no registration fee.

6.8 How frequently must registrations/notifications be renewed (if applicable)?

Registrations/notifications must be renewed when any amendments are made.

6.9 Is any prior approval required from the data protection regulator?

Yes, prior approval is required for disclosure of personal data processed according to the specific provision in the DP Act on processing personal data for the sole purpose of statistical or scientific studies of significant importance to society. Approval is required when disclosure to a third party is for (i) the purpose of processing outside the territorial scope of the GDPR, (ii) processing that relates to biological material; or (iii) the purpose of publication in a recognised scientific journal or similar, cf. question 6.1.

6.10 Can the registration/notification be completed online?

No, it requires a positive approval from the DPA.

6.11 Is there a publicly available list of completed registrations/notifications?

No, but the application and the authorisation can be subject to requests of subject access according to the Danish Publicity Act.

6.12 How long does a typical registration/notification process take?

It takes a minimum of six months, sometimes longer. There is a very small number of cases at this point.
assessments and the training of staff; and (iv) co-operating with the data protection authority and acting as the authority’s primary contact point for issues related to data processing.

7.7 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?

Yes, the controller or processor must notify the data protection authority of the contact details of the designated Data Protection Officer.

7.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?

The Data Protection Officer does not necessarily need to be named in the public-facing privacy notice. However, the contact details of the Data Protection Officer must be notified to the data subject when personal data relating to that data subject are collected. As a matter of good practice, the Article 29 Working Party (the “WP29”) (now the European Data Protection Board (the “EDPB”)) recommended in its 2017 guidance on Data Protection Officers that both the data protection authority and employees should be notified of the name and contact details of the Data Protection Officer.

8 Appointment of Processors

8.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?

Yes. The business that appoints a processor to process personal data on its behalf, is required to enter into an agreement with the processor which sets out the subject matter for processing, the duration of processing, the nature and purpose of processing, the types of personal data and categories of data subjects and the obligations and rights of the controller (i.e., the business).

It is essential that the processor appointed by the business complies with the GDPR.

8.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?

The processor must be appointed under a binding agreement in writing. The contractual terms must stipulate that the processor: (i) only acts on the documented instructions of the controller; (ii) imposes confidentiality obligations on all relevant employees; (iii) ensures the security of personal data that it processes; (iv) abides by the rules regarding the appointment of sub-processors; (v) implements measures to assist the controller with guaranteeing the rights of data subjects; (vi) assists the controller in obtaining approval from the relevant data protection authority; (vii) either returns or destroys the personal data at the end of the relationship (except as required by EU or Member State law); and (viii) provides the controller with all information necessary to demonstrate compliance with the GDPR.

9 Marketing

9.1 Please describe any legislative restrictions on the sending of electronic direct marketing (e.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?).

According to the Danish Marketing Practices Act, it is required to obtain a prior opt-in consent from the recipient. There are some modifications for customers of the trader.

9.2 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.).

The national opt-out register “Robinsonlisten” must be checked in advance before marketing by telephone and post.

Marketing by telephone is legal without consent, when the sole purpose is to sell:

- Books.
- Subscriptions to newspapers and magazines.
- Insurance.
- Rescue services and healthcare subscriptions.

9.3 Do the restrictions noted above apply to marketing sent from other jurisdictions?

Yes, European and other international traders must comply with the Danish Marketing Practices Act when sending direct marketing to Danish consumers.

9.4 Is/are the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?

The supervision authority of the Marketing Practices Act is the Danish Consumer Ombudsman.

The Danish Consumer Ombudsman is very active in the enforcement of breaches of marketing restrictions.

9.5 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?

Yes, it is lawful to purchase such lists. However, the receiving party must comply with the Marketing Practices Act. The disclosing party shall comply with Section 13 of the DP Act, which states that an enterprise may not disclose data concerning a consumer to another enterprise for the purpose of direct marketing or use such data on behalf of another enterprise for such marketing purpose unless the consumer has given explicit consent. Consent shall be obtained in accordance with the rules laid down in section 10 of the Marketing Practices Act.

On certain conditions, disclosure of general data on customers which form the basis for classification into customer categories may take place without consent. It is a condition that the information can be processed according to Article 6 (1)(f) of the GDPR. It is required that the data controller, prior to disclosure, controls whether the data subjects have opted out of marketing via the opt-out list/Robinsonlisten.
Data controllers who sell lists of groups of persons for direct marketing purposes or who print addresses or distribute messages to such groups on behalf of a third party may only process:

(i) data concerning name, address, position, occupation, e-mail address, telephone and fax number;

(ii) data contained in trade registers which according to law, or provisions laid down by law, are intended for public information; and

(iii) other data if the data subject has given explicit consent. Consent according to Section 13 must be obtained in accordance with section 10 of the Danish Marketing Practices Act.

9.6 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?

When calculating a fine for unlawful direct marketing (spam), the following calculation model applies:

Up to 100 spam mails/SMS will trigger a fine of DKK 10,000. For over 100 spam mail/SMS, a fine of DKK 100 for each mail will be given additionally. Thus, the penalty for 60 spam mails/SMS will be DKK 10,000, and for 140 spam mails/SMS the fine will be DKK 14,000.

However, the starting point could derogate in the upward and downward direction if there are aggravating or mitigating circumstances in the specific case.

In our knowledge, the maximum penalty for sending unlawful direct marketing is DKK 800,000 (approx. EUR 107,200).

10 Cookies

10.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).

In November 2009, the European Commission adopted Directive 2009/136/EC (2009 Directive), which amended Directive 2002/58/EC also known as the e-Privacy Directive. This amendment has been implemented into Danish law by way of Executive Order No. 1148 of 9 December 2011 (the “Cookie Order”).

The Cookie Order implements Article 5 of the ePrivacy Directive. Pursuant to Article 5 of the EU ePrivacy Directive, the storage of cookies (or other data) on an end user’s device requires prior consent (the applicable standard of consent is derived from the GDPR). However, the Danish legal guideline on the Cookie Order accepts passively given consent. For consent to be valid, it must be informed, specific and freely given. This does not apply if: (i) the cookie is for the sole purpose of carrying out the transmission of a communication over an electronic communications network; or (ii) the cookie is strictly necessary to provide an “information society service” (e.g., a service over the internet) requested by the subscriber or user, which means that it must be essential to fulfil their request.

The Executive Order addresses a variety of issues, such as security of processing, disclosure of certain breaches of security, and unsolicited communications. In addition, the 2009 Directive amended Section 5(3) of the 2002 e-Privacy Directive to require that storing information on a user’s computer, or gaining access to information already stored on a user’s computer, be permitted only if the user has previously agreed to such access or storage, and has received clear and comprehensive information about the purpose of this storage or access. Section 5(3) also included exceptions for (i) technical storage or access in connection with the transmission of information over an electronic communication network and (ii) when the use of a cookie is strictly necessary to provide a service explicitly requested by the user.

The Danish Business Authority is the supervisory authority regarding the regulation on the use of cookies. The EU Commission intends to pass a new ePrivacy Regulation that will replace the respective national legislation in the EU Member States. The ePrivacy Regulation is planned to come into force in 2019.

10.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?

Technical cookies which are necessary to perform a service explicitly requested by the user will typically not be covered by the Cookie Order.

Examples of technical necessary cookies include: internet connection; payment gateways; booking systems; Web Forms; and electronic shopping carts on webshops.

10.3 To date, has/have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?

No, the Danish Business Authority has not taken any enforcement action.

10.4 What are the maximum penalties for breaches of applicable cookie restrictions?

This is not applicable – no enforcement has taken place. The level of fines is not capped.

11 Restrictions on International Data Transfers

11.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.

Data transfers to other jurisdictions that are not within the European Economic Area (the “EEA”) can only take place if the transfer is to an “Adequate Jurisdiction” (as specified by the EU Commission), the business has implemented one of the required safeguards as specified by the GDPR, or one of the derogations specified in the GDPR applies to the relevant transfer. The EDPB Guidelines (2/2018) set out that a “layered approach” should be taken with respect to these transfer mechanisms. If the transfer is not to an Adequate Jurisdiction, the data exporter should first explore the possibility of implementing the safeguards provided for in the GDPR before relying on a derogation.

11.2 Please describe the mechanisms businesses typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).

When transferring personal data to a country other than an Adequate Jurisdiction, businesses must ensure that there are appropriate safeguards on the data transfer, as prescribed by the GDPR. The
GDPR offers a number of ways to ensure compliance for international data transfers, of which one is consent of the relevant data subject. Other common options are the use of Standard Contractual Clauses or BCRs. Businesses can adopt the Standard Contractual Clauses drafted by the EU Commission – these are available for transfers between controllers, and transfers between a controller (as exporter) and a processor (as importer). International data transfers may also take place on the basis of contracts agreed between the data exporter and data importer provided that they conform to the protections outlined in the GDPR, and they have prior approval by the relevant data protection authority.

International data transfers within a group of businesses can be safeguarded by the implementation of Binding Corporate Rules (“BCRs”). The BCRs will always need approval from the relevant data protection authority. Most importantly, the BCRs will need to include a mechanism to ensure they are legally binding and enforced by every member in the group of businesses. Among other things, the BCRs must set out the group structure of the businesses, the proposed data transfers and their purpose, the rights of data subjects, the mechanisms that will be implemented to ensure compliance with the GDPR and the relevant compliant procedures. Transfer of personal data to the USA is also possible if the data importer has signed up to the EU-US Privacy Shield Framework, which was designed by the US Department of Commerce and the EU Commission to provide businesses in the EU and the US with a mechanism to comply with data protection requirements when transferring personal data from the EU to the US.

11.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.

It is likely that the international data transfer will require prior approval from the relevant data protection authority unless they have already established a GDPR compliant mechanism as set out above for such transfers.

In any case, most of the safeguards outlined in the GDPR will need initial approval from the data protection authority, such as the establishment of BCRs.

See also question 6.9.

12 Whistle-blower Hotlines

12.1 What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.?)?

Internal whistle-blowing schemes are generally established in pursuance of a concern to implement proper corporate governance principles in the daily functioning of businesses. Whistle-blowing is designed as an additional mechanism for employees to report misconduct internally through a specific channel and supplements a business’ regular information and reporting channels, such as employee representatives, line management, quality-control personnel or internal auditors who are employed precisely to report such misconduct.

The WP29 has limited its Opinion 1/2006 on the application of EU data protection rules to internal whistle-blowing schemes to the fields of accounting, internal accounting controls, auditing matters, fight against bribery, banking and financial crime. The scope of corporate whistle-blower hotlines, however, does not need to be limited to any particular issues. In the Opinion it is recommended that the business responsible for the whistle-blowing scheme should carefully assess whether it might be appropriate to limit the number of persons eligible for reporting alleged misconduct through the whistle-blowing scheme and whether it might be appropriate to limit the number of persons who may be reported through the scheme, in particular in the light of the seriousness of the alleged offences reported. According to the former Danish Act on Processing of Personal Data, the DPA issued a guideline on processing of personal data in connection with whistleblower systems. According to the guideline, a company may process information relating to corporate crime, safety at work issues, and violation of rules that may have a serious consequence for employees such as sexual harassment or violence. Additionally, information that it would be mandatory to report under the US Sarbanes-Oxley Act may, in the opinion of the DPA, be legally processed in a whistleblower system. Special categories of information, such as information pertaining to an employee’s criminal records, may be processed. However, sensitive information as of Article 9 of the GDPR may not be processed. According to several corporate rules, some entities are obliged to establish whistle-blower schemes. The DPA approves that these types of whistle-blower schemes may be legally processed.

12.2 Is anonymous reporting prohibited, strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do businesses typically address this issue?

Anonymous reporting is not prohibited under EU data protection law; however, it raises problems as regards the essential requirement that personal data should only be collected fairly. In Opinion 1/2006, the WP29 considered that only identified reports should be advertised in order to satisfy this requirement. Businesses should not encourage or advertise the fact that anonymous reports may be made through a whistleblower scheme. An individual who intends to report to a whistleblower system should be aware that he/she will not suffer due to his/her action. The whistleblower, at the time of establishing the first contact with the scheme, should be informed that his/her identity will be kept confidential at all the stages of the process, and in particular will not be disclosed to third parties, such as the incriminated person or to the employee’s line management. If, despite this information, the person reporting to the scheme still wants to remain anonymous, the report will be accepted into the scheme. Whistle-blowers should be informed that their identity may need to be disclosed to the relevant people involved in any further investigation or subsequent judicial proceedings instigated as a result of any enquiry conducted by the whistleblower scheme.

13 CCTV

13.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?

A data protection impact assessment (“DPIA”) must be undertaken with assistance from the Data Protection Officer when there is a
systematic monitoring of a publicly accessible area on a large scale. If the DPIA suggests that the processing would result in a high risk to the rights and freedoms of individuals prior to any action being taken by the controller, the controller must consult the data protection authority.

During the course of a consultation, the controller must provide information on the responsibilities of the controller and/or processors involved, the purpose of the intended processing, a copy of the DPIA, the safeguards provided by the GDPR to protect the rights and freedoms of data subjects and where applicable, the contact details of the Data Protection Officer.

If the data protection authority is of the opinion that the CCTV monitoring would infringe the GDPR, it has to provide written advice to the controller within eight weeks of the request of a consultation and can use any of its wider investigative, advisory and corrective powers outlined in the GDPR.

The Danish Act no. 1190 of 11 October 2007 regarding CCTV is supervised by the Danish National Police. The act regulates private controllers’ use of CCTV. The act has specific provisions regarding the transfer of personal data from CCTV. The act does not regulate where and in which cases public authorities can initiate CCTV, which is governed by the GDPR and the DP Act.

13.2 Are there limits on the purposes for which CCTV data may be used?

Yes, only for the purpose of preventing crime and for security purposes.

14 Employee Monitoring

14.1 What types of employee monitoring are permitted (if any), and in what circumstances?

Employees can be monitored when the following conditions are met:

■ The monitoring is justified for operational reasons and according to a fair purpose.
■ The monitoring is not offensive to the employees.
■ The monitoring does not cause losses or significant disadvantages.
■ The monitoring is proportional according to its purpose.
■ The employee shall be given six weeks’ notice. If the purpose or operational reasons make it necessary, monitoring can be initiated without notice.

Examples of employee monitoring include e-mail and internet access, CCTV, time recorders, etc.

14.2 Is consent or notice required? Describe how employers typically obtain consent or provide notice.

Notice is required, and the notice is typically given in connection with the employment agreement.

14.3 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?

If the company has a work council, such work council should be notified; alternatively, the union representative.

It is recommended that an actual local agreement be concluded on the control measures and on any consequences of an infringement.

15 Data Security and Data Breach

15.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?

Yes. Personal data must be processed in a way which ensures security and safeguards against unauthorised or unlawful processing, accidental loss, destruction and damage of the data.

Both controllers and processors must ensure they have appropriate technical and organisational measures to meet the requirements of the GDPR. Depending on the security risk, this may include the encryption of personal data, the ability to ensure the ongoing confidentiality, integrity and resilience of processing systems, an ability to restore access to data following a technical or physical incident and a process for regularly testing and evaluating the technical and organisational measures for ensuring the security of processing.

15.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

The controller is responsible for reporting a personal data breach without undue delay (and in any case within 72 hours of first becoming aware of the breach) to the relevant data protection authority, unless the breach is unlikely to result in a risk to the rights and freedoms of the data subject(s). A processor must notify any data breach to the controller without undue delay.

The notification must include the nature of the personal data breach including the categories and number of data subjects concerned, the name and contact details of the Data Protection Officer or relevant point of contact, the likely consequences of the breach and the measures taken to address the breach including attempts to mitigate possible adverse effects.

15.3 Is there a legal requirement to report data breaches to affected data subjects? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

Controllers have a legal requirement to communicate the breach to the data subject, without undue delay, if the breach is likely to result in a high risk to the rights and freedoms of the data subject.

The notification must include the name and contact details of the Data Protection Officer (or other point of contact), the likely consequences of the breach and any measures taken to remedy or mitigate the breach.

The controller may be exempt from notifying the data subject if the risk of harm is remote (e.g., because the affected data is encrypted), the controller has taken measures to minimise the risk of harm (e.g., suspending affected accounts) or the notification requires a disproportionate effort (e.g., a public notice of the breach).
15.4 What are the maximum penalties for data security breaches?

The maximum penalty is the higher of €20 million or 4% of worldwide turnover.

16 Enforcement and Sanctions

16.1 Describe the enforcement powers of the data protection authority(ies).

<table>
<thead>
<tr>
<th>Investigatory Power</th>
<th>Civil/Administrative Sanction</th>
<th>Criminal Sanction</th>
</tr>
</thead>
<tbody>
<tr>
<td>Investigative Powers</td>
<td>The data protection authority has wide powers to order the controller and the processor to provide any information it requires for the performance of its tasks, to conduct investigations in the form of data protection audits, to carry out review on certificates issued pursuant to the GDPR, to notify the controller or processor of alleged infringement of the GDPR, to access all personal data and all information necessary for the performance of controllers’ or processors’ tasks and access to the premises of the data including any data processing equipment.</td>
<td>N/A</td>
</tr>
<tr>
<td>Corrective Powers</td>
<td>The data protection authority has a wide range of powers including to issue warnings or reprimands for non-compliance, to order the controller to disclose a personal data breach to the data subject, to impose a permanent or temporary ban on processing, to withdraw a certification and to recommend a fine (as below).</td>
<td>N/A</td>
</tr>
<tr>
<td>Authorisation and Advisory Powers</td>
<td>The data protection authority has a wide range of powers to advise the controller, accredit certification bodies and to authorise certificates, contractual clauses, administrative arrangements and binding corporate rules as outlined in the GDPR. The opinion of the DPA shall be obtained of legislative proposals, executive orders, circulars or similar general regulations that affect the protection of privacy in connection with the processing of personal data.</td>
<td>N/A</td>
</tr>
<tr>
<td>Imposition of administrative fines for infringements of specified GDPR provisions</td>
<td>The legal system of Denmark does not allow for administrative fines as set out in the GDPR. However, the GDPR states that the competent national courts should take into account the recommendation by the supervisory authority initiating the fine. In any event, the fines imposed should be effective, proportionate and dissuasive. The GDPR provides for administrative fines which can be €20 million or up to 4% of the business’ worldwide annual turnover of the proceeding financial year, and the Danish courts are bound by this.</td>
<td>N/A</td>
</tr>
<tr>
<td>Non-compliance with a data protection authority</td>
<td>As mentioned above, the legal systems of Denmark do not allow for administrative fines as set out in the GDPR. Therefore, the DPA may not impose fines for non-compliance, but could instead recommend a fine with the national courts. Also, the DPA may file a civil case with the Danish courts.</td>
<td>N/A</td>
</tr>
</tbody>
</table>

16.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?

The GDPR entitles the relevant data protection authority to impose a temporary or definitive limitation including a ban on processing. The DP Act may in exceptional cases prohibit, restrict, or suspend the transfer to a third country or an international organisation of information according to Article 9(1) of the GDPR in cases where a decision has not been adopted concerning the adequacy of the level of protection under Article 45 of the GDPR.

16.3 Describe the data protection authority’s approach to exercising those powers, with examples of recent cases.

DPA has issued an order for DK Hostmaster (the Danish registry of .dk domain names) to stop the disclosure of certain information on its website. The DPA has filed a police report regarding a Danish taxi company. The DPA has recommended a fine of DKK 1.2 million (approx. EUR 160,756.60) for a violation of the rules in the GDPR. The violation regards lack of deletion and proper information of the data subjects. Around 9 million taxi trips were unlawfully processed. This is the first time the DPA has recommended a fine according to the GDPR.

16.4 Does the data protection authority ever exercise its powers against businesses established in other jurisdictions? If so, how is this enforced?

The one-stop shop mechanism of the GDPR will regulate cases where the Danish DPA has jurisdiction in another Member State. To our knowledge, the one-stop shop is still at a testing stage between the European Data Protection Authorities.

17 E-discovery / Disclosure to Foreign Law Enforcement Agencies

17.1 How do businesses typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?

Foreign law enforcement authorities requesting information from Danish entities, etc. must send a letter rogatory to the Danish law enforcement authorities regarding the information needed. In this case, the Danish law enforcement authorities may try to get a court order or to obtain acknowledgment of a foreign court order. A Danish data controller is only permitted to disclose personal data according to the regulation on processing of personal data (primarily, the GDPR or the DP Act).

17.2 What guidance has/have the data protection authority(ies) issued?

There is no specific guidance on the subject.
18 Trends and Developments

18.1 What enforcement trends have emerged during the previous 12 months? Describe any relevant case law.

Please refer to question 16.3.

Sissel Kristensen
Integra Law Firm
1050 Copenhagen K
Denmark
Tel: +45 52 50 06 44
Email: sis@integralaw.dk
URL: www.integralaw.dk

Sissel specialises in privacy and marketing law. Sissel has a background as head of section with the Danish Data Protection Agency, where she worked on the enforcement of data protection rules in connection with national and international audits, the processing of personal data by public authorities and private businesses, as well participating in preparatory legislative work. In addition, Sissel has given lectures on European and national privacy law.

Heidi Højmark Helveg
Integra Law Firm
1050 Copenhagen K
Denmark
Tel: +45 30 74 29 00
Email: hhh@integralaw.dk
URL: www.integralaw.dk

Heidi specialises in marketing law, privacy law/GDPR and intellectual property law.

In recent years, she has focused on providing advice relating to marketing law, personal data law and media law, and over the years, she has also gained solid expertise in intellectual property law (especially trademark law and copyright law). She represents Danish and international companies, organisations and public authorities. Her experience in marketing law was enhanced when she was appointed member of the Danish Government’s Marketing Law Commission at the end of 2014, upon recommendation by the Association of Danish Law Firms and the Danish Bar and Law Society.

18.2 What “hot topics” are currently a focus for the data protection regulator?

Data minimisation has been subject to two cases of a larger scale. One of the cases is referred to in question 16.3.
Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

Since 25 May 2018, the principal data protection legislation in the EU has been Regulation (EU) 2016/679 (the “General Data Protection Regulation” or “GDPR”). The GDPR repealed Directive 95/46/EC (the “Data Protection Directive”) and has led to increased (though not total) harmonisation of data protection law across the EU Member States.

On June 2018, the French parliament voted on a new law to include and complete the transposition of the GDPR into the French system (bearing in mind that the GDPR is applicable per se); this “new” French law was published on and became effective as of 21 June 2018, and will be further completed by a decree redrafting law n° 78-17 dated 6 January 1978.

1.2 Is there any other general legislation that impacts data protection?

The French post and electronic communications code includes article L. 34-5, which prevents the sending of fax and emails to consumers without their prior consent, in accordance with the requirements of Directive 2002/58/EC (as amended by Directive 2009/136/EC) (the “ePrivacy Directive”). In January 2017, the European Commission published a proposal for an ePrivacy Regulation that would harmonise the applicable rules across the EU.

The EU Directive on the Security of Network and Information Systems (NIS) reinforces the obligation as set out in the GDPR to take technical and organisational measures to secure technology, data and networks (“Systems”). Indeed, the NIS Directive places obligations on organisations in essential industries to secure their Systems and to take steps to protect said Systems against cyber threats. The NIS Directive was implemented in France on 6 February 2019 by French Law n° 2018-133 on the various provisions adapted to European Union law on matters of security.


1.3 Is there any sector-specific legislation that impacts data protection?

The French authority responsible for data protection – the National Commission for Computing and Freedom, i.e. Commission Nationale de l’Informatique et des Libertés, “CNIL,” – may issue guidelines with regard to the processing of genetic data, biometric data or data concerning health, in accordance with article 9 (4) of the GDPR.

1.4 What authority(ies) are responsible for data protection?

The CNIL is the French body responsible for data protection.

Definitions

2.1 Please provide the key definitions used in the relevant legislation:

- “Personal Data” means any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
- “Processing” means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
- “Controller” means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
- “Processor” means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
- “Data Subject” means an individual who is the subject of the relevant personal data.
- “Sensitive Personal Data” are personal data, revealing racial or ethnic origin, political opinions, religious or philosophical...
beliefs, trade-union membership, data concerning health or sex life and sexual orientation, genetic data or biometric data.

“Data Breach” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

3 Territorial Scope

3.1 Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to those laws?

The GDPR applies to businesses that are established in any EU Member State, and that process personal data (either as a controller or processor, and regardless of whether or not the processing takes place in the EU) in the context of that establishment.

A business that is not established in any Member State, but is subject to the laws of a Member State by virtue of public international law, is also subject to the GDPR.

The GDPR applies to businesses outside the EU if they (either as controller or processor) process the personal data of EU residents in relation to: (i) the offering of goods or services (whether or not in return for payment) to EU residents; or (ii) the monitoring of the behaviour of EU residents (to the extent that such behaviour takes place in the EU).

Further, the GDPR applies to businesses established outside the EU if they monitor the behaviour of EU residents (to the extent such behaviour takes place in the EU).

Additional French regulation on personal data applies to individuals residing in France, except for processing carried out for journalistic purposes or for the purpose of academic, artistic or literary expression, which shall be subject to the home state law of the controller.

4 Key Principles

4.1 What are the key principles that apply to the processing of personal data?

- **Transparency**
  Personal data must be processed lawfully, fairly and in a transparent manner. Controllers must provide certain minimum information to data subjects regarding the collection and further processing of their personal data. Such information must be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

- **Lawful basis for processing**
  Processing of personal data is lawful only if, and to the extent that, it is permitted under EU data protection law. The GDPR provides an exhaustive list of legal bases on which personal data may be processed, of which the following are the most relevant for businesses: (i) prior, freely given, specific, informed and unambiguous consent of the data subject; (ii) contractual necessity (i.e., the processing is necessary for the performance of a contract to which the data subject is a party, or for the purposes of pre-contractual measures taken at the data subject’s request); (iii) compliance with legal obligations (i.e., the controller has a legal obligation, under the laws of the EU or an EU Member State, to perform the relevant processing); (iv) legitimate interests (i.e., the processing is necessary for the purposes of legitimate interests pursued by the controller, except where the controller’s interest are overridden by the interests, fundamental rights or freedoms of the affected data subjects); (v) vital interests (i.e., the processing is necessary to protect someone’s life); or (vi) public task (i.e., the processing is necessary for the controller to perform a task in the public interest or for its official functions, and the task or function has a clear basis in law).

Please note that businesses require stronger grounds to process sensitive personal data. The processing of sensitive personal data is only permitted under certain conditions, of which the most relevant for businesses are: (i) explicit consent of the affected data subject; (ii) the processing is necessary in the context of employment law; or (iii) the processing is necessary for the establishment, exercise or defence of legal claims.

- **Purpose limitation**
  Personal data may only be collected for specified, explicit and legitimate purposes and must not be further processed in a manner that is incompatible with those purposes. If a controller wishes to use the relevant personal data in a manner that is incompatible with the purposes for which they were initially collected, it must: (i) inform the data subject of such new processing; and (ii) must be able to rely on a lawful basis as set out above.

- **Data minimisation**
  Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which those data are processed. A business should only process the personal data that it actually needs to process in order to achieve its processing purposes.

- **Accuracy**
  Personal data must be accurate and, where necessary, kept up to date. A business must take every reasonable step to ensure that personal data that are inaccurate are either erased or rectified without delay.

- **Retention**
  Personal data must be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

- **Data security**
  Personal data must be processed in a manner that ensures appropriate security of those data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

- **Accountability**
  The controller is responsible for, and must be able to demonstrate, compliance with the data protection principles set out above.

5 Individual Rights

5.1 What are the key rights that individuals have in relation to the processing of their personal data?

- **Right of access to data/copies of data**
  A data subject has the right to obtain from a controller the following information in respect of the data subject’s personal data: (i) confirmation of whether, and where, the controller is processing the data subject’s personal data; (ii) information about the purposes of the processing; (iii) information about the categories of data being processed; (iv) information about the categories of recipients with whom the data may be shared; (v) information about the period for which the data will be stored (or the criteria used to determine that period); (vi) information about the existence of the rights to erasure, to rectification, to restriction of processing and to...
object to processing; (vii) information about the existence of the right to complain to the relevant data protection authority; (viii) where the data were not collected from the data subject, information as to the source of the data; and (ix) information about the existence of, and an explanation of the logic involved in, any automated processing that has a significant effect on the data subject.

Additionally, the data subject may request a copy of the personal data being processed.

- **Right to rectification of errors**
  Controllers must ensure that inaccurate or incomplete data are erased or rectified. Data subjects have the right to rectification of inaccurate personal data.

- **Right to deletion/right to be forgotten**
  Data subjects have the right to erasure of their personal data (the “right to be forgotten”) if: (i) the data are no longer needed for their original purpose (and no new lawful purpose exists); (ii) the lawful basis for the processing is the data subject’s consent, the data subject withdraws that consent, and no other lawful ground exists; (iii) the data subject exercises the right to object, and the controller has no overriding grounds for continuing the processing; (iv) the data have been processed unlawfully; or (v) erasure is necessary for compliance with EU law or national data protection law.

- **Right to object to processing**
  Data subjects have the right to object, on grounds relating to their particular situation, to the processing of personal data where the basis for that processing is either public interest or legitimate interest of the controller. The controller must cease such processing unless it demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the relevant data subject or requires the data in order to establish, exercise or defend legal rights.

- **Right to restrict processing**
  Data subjects have the right to restrict the processing of personal data, which means that the data may only be held by the controller, and may only be used for limited purposes if: (i) the accuracy of the data is contested (and only for as long as it takes to verify that accuracy); (ii) the processing is unlawful and the data subject requests restriction (as opposed to exercising the right to erasure); (iii) the controller no longer needs the data for their original purpose, but the data are still required by the controller to establish, exercise or defend legal rights; or (iv) verification of overriding grounds is pending, in the context of an erasure request.

- **Right to data portability**
  Data subjects have a right to receive a copy of their personal data in a commonly used machine-readable format, and transfer their personal data from one controller to another or have the data transmitted directly between controllers.

- **Right to withdraw consent**
  A data subject has the right to withdraw their consent at any time. The withdrawal of consent does not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject must be informed of the right to withdraw consent. It must be as easy to withdraw consent as to give it.

- **Right to object to marketing**
  Data subjects have the right to object to the processing of personal data for the purpose of direct marketing, including profiling.

- **Right to complain to the relevant data protection authority(ies)**
  Data subjects have the right to lodge complaints concerning the processing of their personal data with CNIL, if the data subjects lives in France or the alleged infringement occurred in France.

---

**6 Registration Formalities and Prior Approval**

### 6.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?

Before the GDPR, companies acting in France had to notify the French control authority that they were dealing with personal data. With the introduction of the GDPR, this obligation has been withdrawn and the controller now instead has the obligation to hold a record of processing activities in accordance with articles 30 and 31 of the GDPR (accountability principle – see question 4.1).

The obligation to hold records shall not apply to an enterprise employing fewer than 250 persons unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing includes special categories of data (as defined by articles 9 and 10 of the GDPR) or the processing is not occasional.

With regards to French law n°78-17 as amended, prior approval still exists for the processing of personal data on the legal basis of public task and for automated data processing for study or research purposes in the health sector and the evaluation or analysis of practices or activities of care or prevention.

According to the amended law n°78-17, collecting data concerning health will not need prior approval by the CNIL but will have to be done in accordance with the framework approved by the CNIL and l’Institut national des données de santé – article 13 – and in accordance with one of the exceptions that allow the processing of special categories of personal data (article 9.2 of the GDPR).

For the next 10 years, the existing list of personal data registered with the CNIL will be accessible to the public (https://www.cnil.fr/fr/les-formalites-prealables-accomplices-aupres-de-la-cnil-avant-le-25-mai-2018).

### 6.2 If such registration/notification is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?

Any processing that has been notified to the CNIL prior to 25 May 2018 does not need to be accompanied with a DPIA for three years starting from 25 May 2018, unless there has been a substantial change since said notification.

### 6.3 On what basis are registrations/notifications made (e.g., per legal entity, per processing purpose, per data category, per system or database)?

Notifications are made on the basis of the processing purpose and the data category.
6.4 Who must register with/notify the data protection authority (e.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation)?

The data controller (as defined in the GDPR – article 4) shall notify the data protection authority, even when the processing is carried out by a processor.

6.5 What information must be included in the registration/notification (e.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes)?

The information that must be provided includes details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes, transfers outside the EU, rights of data subjects and security measures.

6.6 What are the sanctions for failure to register/notify where required?

See question 6.1 above.

6.7 What is the fee per registration/notification (if applicable)?

Notification is free of charge.

6.8 How frequently must registrations/notifications be renewed (if applicable)?

See question 6.1 above.

6.9 Is any prior approval required from the data protection regulator?

See question 6.1 above.

6.10 Can the registration/notification be completed online?

See question 6.1 above.

6.11 Is there a publicly available list of completed registrations/notifications?

Yes, the CNIL holds a publicly available list of completed registrations/notifications that were finalised prior to 25 May 2018.

6.12 How long does a typical registration/notification process take?

See question 6.1 above.

7 Appointment of a Data Protection Officer

7.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.

The appointment of a Data Protection Officer for controllers or processors is only mandatory in some circumstances including where there is: (i) large-scale regular and systematic monitoring of individuals; or (ii) large-scale processing of sensitive personal data. Where a business designates a Data Protection Officer voluntarily, the requirements of the GDPR apply as though the appointment were mandatory.

7.2 What are the sanctions for failing to appoint a Data Protection Officer where required?

In the circumstances where appointment of a Data Protection Officer is mandatory, failure to comply may result in the wide range of penalties available under the GDPR.

7.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect of his or her role as a Data Protection Officer?

The appointed Data Protection Officer should not be dismissed or penalised for performing their tasks and should report directly to the highest management level of the controller or processor.

7.4 Can a business appoint a single Data Protection Officer to cover multiple entities?

A single Data Protection Officer is permitted by a group of undertakings provided that the Data Protection Officer is easily accessible from each establishment.

7.5 Please describe any specific qualifications for the Data Protection Officer required by law.

The Data Protection Officer should be appointed on the basis of professional qualities and should have an expert knowledge of data protection law and practices. While this is not strictly defined, it is clear that the level of expertise required will depend on the circumstances. For example, the involvement of large volumes of sensitive personal data will require a higher level of knowledge. The CNIL plans to appoint a certification body which will be empowered to deliver Data Protection Officer certification. A French association of Data Protection Officers (L’Association française des correspondants à la protection des données à caractère personnel – www.afcdp.net) has drafted a charter of ethics for Data Protection Officers; Data Protection Officers may choose whether to adhere to this charter.

7.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?

A Data Protection Officer should be involved in all issues which relate to the protection of personal data. The GDPR outlines the minimum
Please describe any legislative restrictions on the marketing of personal data (e.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?).

Prior authorisation shall be expressly obtained before sending direct marketing to consumers (see article L. 34-5 of the French post and electronic communications code regarding fax and emails). Any consumer receiving telephone or SMS spam may transfer them to “33 700” and block the telephone or SMS spam.

Any consumer may register in a list of opposition to out-bound calls, called Bloctel (www.bloctel.gouv.fr). The registration on that list is for a period of three years and may be renewed every three years. Companies are forbidden to call consumers registered on this list, unless (i) the consumer was a previous client of the company, (ii) the company is selling subscriptions to newspapers or magazines, or (iii) the company is a polling institute or a non-profit organisation for a non-commercial purpose.

In the event of previous relationships between the company and the consumer:
- The company shall nevertheless inform the consumer that he/she may decline its opposition to future marketing calls.
- The company is no longer entitled to call the consumer after the end of the concerned service (e.g., the purchased good was delivered), if the consumer is registered on the Bloctel list.

If the consumer has communicated his/her phone number to be called back, the company is only entitled to call this number within three months of the communication of the phone number.

The GDPR protects the persons residing within the EU. EU citizens must agree to receive marketing emails. In this regard, marketing sent from other jurisdictions should comply with EU regulations concerning the sending of marketing emails from other jurisdictions.

The consumer may file a claim online with Bloctel against companies calling him/her in breach of his/her registration on that list (www.bloctel.gouv.fr) or with the CNIL relating to telephone or SMS spam.
9.5 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?

The purchase of lists from third parties is lawful. However, the purchaser of the list shall ensure that the seller of the lists has obtained the express agreement of consumers that their data be transferred to third parties and must check that the phone number is not registered on the Bloctel list.

9.6 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?

The maximum criminal penalties are five years’ imprisonment and a fine of €300,000 (for individuals) or €1.5 million (if the company is held liable). In addition, a maximum administrative fine of €20 million may be imposed by the CNIL for failure to comply with GDPR requirements (see question 16.1 below).

10 Cookies

10.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).

Article 32, II of French law n°78-17, dated 6 January 1978, implements Article 5 of the ePrivacy Directive. Pursuant to Article 5 of the EU ePrivacy Directive, the storage of cookies (or other data) on an end user’s device requires prior consent (the applicable standard of consent is derived from the GDPR). For consent to be valid, it must be informed, specific, freely given and must constitute a real and unambiguous indication of the individual’s wishes. This does not apply if: (i) the cookie is for the sole purpose of carrying out the transmission of a communication over an electronic communications network; or (ii) the cookie is strictly necessary to provide an “information society service” (e.g., a service over the internet) requested by the subscriber or user, which means that it must be essential to fulfil their request.

The EU Commission intends to pass a new ePrivacy Regulation that will replace the respective national legislation in the EU Member States. The ePrivacy Regulation is planned to come into force in 2019.

10.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?

See question 10.1 above.

10.3 To date, has/have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?

The French control authority CNIL has issued rules concerning cookies, which are close to the ones issued by the WP29: the prior consent of the person visiting a website shall be obtained (subject to exceptions: see question 10.1 above); this prior consent is valid for 13 months (see www.cnil.fr/fr/cookies).

In the course of 2016, the CNIL launched an inquiry over 13 websites concerning their use of cookies.

On 23 March 2017, the CNIL sentenced a major web company to a €150,000 penalty for lack of information of the users of its website concerning cookies used by this website and the impossibility to refuse cookies.

On 18 May 2017, the CNIL imposed a financial penalty of €25,000 on the website Challenges.fr for failure to provide information, failure to implement a valid opposition mechanism to the deposit of cookies on the user’s terminal, no definition and non-compliance with a data retention period proportionate to the purpose of the processing.

The penalties in relation to cookies are usually linked to the obligation to inform and the lack of valid consent. Indeed, the main legal basis for processing data in relation to cookies is the data subject’s consent.

10.4 What are the maximum penalties for breaches of applicable cookie restrictions?

The CNIL may impose a maximum administrative fine of €3 million or €20 million, depending on the future interpretation of the scope of GDPR (see question 16.1 below).

On 21 January 2019, the CNIL’s restricted committee imposed a financial penalty of €50 million on the company GOOGLE LLC, in accordance with the GDPR, for lack of transparency, inadequate information and lack of valid consent regarding advert personalisation (https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc).

11 Restrictions on International Data Transfers

11.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.

Data transfers to other jurisdictions that are not within the European Economic Area (the “EEA”) can only take place if the transfer is to an “Adequate Jurisdiction” (as specified by the EU Commission), the business has implemented one of the required safeguards as specified by the GDPR, or one of the derogations specified in the GDPR applies to the relevant transfer. The EDPB Guidelines (2/2018) set out that a “layered approach” should be taken with respect to these transfer mechanisms. If the transfer is not to an Adequate Jurisdiction, the data exporter should first explore the possibility of implementing one of the safeguards provided for in the GDPR before relying on a derogation.

11.2 Please describe the mechanisms businesses typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).

When transferring personal data to a country other than an Adequate Jurisdiction, businesses must ensure that there are appropriate safeguards on the data transfer, as prescribed by the GDPR. The GDPR offers a number of ways to ensure compliance for international data transfers, of which one is consent of the relevant data subject. Other common options are the use of Standard Contractual Clauses or BCRs.

Businesses can adopt the Standard Contractual Clauses drafted by the EU Commission – these are available for transfers between controllers, and transfers between a controller (as exporter) and a processor (as...
The use of CCTV requires separate registration/notification or prior approval from the relevant data protection authority. This is due to the systematic monitoring of a publicly accessible area on a large scale.

Anonymous reporting is not prohibited under EU data protection law; however, it raises problems as regards the essential requirement that personal data should only be collected fairly. In Opinion 1/2006, the WP29 considered that only identified reports should be advertised in order to satisfy this requirement. Businesses should not encourage or advertise the fact that anonymous reports may be made through a whistle-blower scheme.

An individual who intends to report to a whistle-blowing system should be aware that he/she will not suffer due to his/her action. The whistle-blower, at the time of establishing the first contact with the scheme, should be informed that his/her identity will be kept confidential at all the stages of the process, and in particular will not be disclosed to third parties, such as the incriminated person or to the employee’s line management. If, despite this information, the person reporting to the scheme still wants to remain anonymous, the report will be accepted into the scheme. Whistle-blowers should be informed that their identity may need to be disclosed to the relevant people involved in any further investigation or subsequent judicial proceedings instigated as a result of any enquiry conducted by the whistle-blowing scheme.

Internal whistle-blowing schemes are generally established in pursuance of a concern to implement proper corporate governance principles in the daily functioning of businesses. Whistle-blowing is designed as an additional mechanism for employees to report misconduct internally through a specific channel and supplements a business’s regular information and reporting channels, such as employee representatives, line management, quality-control personnel or internal auditors who are employed precisely to report such misconduct.

The WP29 has limited its Opinion 1/2006 on the application of EU data protection rules to internal whistle-blowing schemes to the fields of accounting, internal accounting controls, auditing matters, and the fight against bribery, banking and financial crime. The scope of corporate whistle-blower hotlines, however, does not need to be limited to any particular issues. In the Opinion, it is recommended that the business responsible for the whistle-blowing scheme should carefully assess whether it might be appropriate to limit the number of persons eligible for reporting alleged misconduct through the whistle-blowing scheme and whether it might be appropriate to limit the number of persons who may be reported through the scheme, in particular in the light of the seriousness of the alleged offences reported.

Under French law, some provisions protect whistle-blowers against any discrimination regarding their salary, professional evolution with regards to conflict of interest concerning a state representative, corruption (article L. 1132-3-3 of the French labour code), serious risk to the health, the environment or the safety of sanitary or cosmetic products, moral or sexual harassment (articles L. 1152-1 and further and article L. 1153-1 and further of the French labour code), discrimination (article L. 1132-3 of the French labour code), serious danger for his/her life or health, defective protection systems (article L. 4131-1 of the French labour code). No specific provision is dedicated to the protection of personal data.

Anonymous reporting is not prohibited under EU data protection law; however, it raises problems as regards the essential requirement that personal data should only be collected fairly. In Opinion 1/2006, the WP29 considered that only identified reports should be advertised in order to satisfy this requirement. Businesses should not encourage or advertise the fact that anonymous reports may be made through a whistle-blower scheme.

An individual who intends to report to a whistle-blowing system should be aware that he/she will not suffer due to his/her action. The whistle-blower, at the time of establishing the first contact with the scheme, should be informed that his/her identity will be kept confidential at all the stages of the process, and in particular will not be disclosed to third parties, such as the incriminated person or to the employee’s line management. If, despite this information, the person reporting to the scheme still wants to remain anonymous, the report will be accepted into the scheme. Whistle-blowers should be informed that their identity may need to be disclosed to the relevant people involved in any further investigation or subsequent judicial proceedings instigated as a result of any enquiry conducted by the whistle-blowing scheme.

Internal whistle-blowing schemes are generally established in pursuance of a concern to implement proper corporate governance principles in the daily functioning of businesses. Whistle-blowing is designed as an additional mechanism for employees to report misconduct internally through a specific channel and supplements a business’s regular information and reporting channels, such as employee representatives, line management, quality-control personnel or internal auditors who are employed precisely to report such misconduct.

The WP29 has limited its Opinion 1/2006 on the application of EU data protection rules to internal whistle-blowing schemes to the fields of accounting, internal accounting controls, auditing matters, and the fight against bribery, banking and financial crime. The scope of corporate whistle-blower hotlines, however, does not need to be limited to any particular issues. In the Opinion, it is recommended that the business responsible for the whistle-blowing scheme should carefully assess whether it might be appropriate to limit the number of persons eligible for reporting alleged misconduct through the whistle-blowing scheme and whether it might be appropriate to limit the number of persons who may be reported through the scheme, in particular in the light of the seriousness of the alleged offences reported.

Under French law, some provisions protect whistle-blowers against any discrimination regarding their salary, professional evolution with regards to conflict of interest concerning a state representative, corruption (article L. 1132-3-3 of the French labour code), serious risk to the health, the environment or the safety of sanitary or cosmetic products, moral or sexual harassment (articles L. 1152-1 and further and article L. 1153-1 and further of the French labour code), discrimination (article L. 1132-3 of the French labour code), serious danger for his/her life or health, defective protection systems (article L. 4131-1 of the French labour code). No specific provision is dedicated to the protection of personal data.

Anonymous reporting is not prohibited under EU data protection law; however, it raises problems as regards the essential requirement that personal data should only be collected fairly. In Opinion 1/2006, the WP29 considered that only identified reports should be advertised in order to satisfy this requirement. Businesses should not encourage or advertise the fact that anonymous reports may be made through a whistle-blower scheme.

An individual who intends to report to a whistle-blowing system should be aware that he/she will not suffer due to his/her action. The whistle-blower, at the time of establishing the first contact with the scheme, should be informed that his/her identity will be kept confidential at all the stages of the process, and in particular will not be disclosed to third parties, such as the incriminated person or to the employee’s line management. If, despite this information, the person reporting to the scheme still wants to remain anonymous, the report will be accepted into the scheme. Whistle-blowers should be informed that their identity may need to be disclosed to the relevant people involved in any further investigation or subsequent judicial proceedings instigated as a result of any enquiry conducted by the whistle-blowing scheme.

Internal whistle-blowing schemes are generally established in pursuance of a concern to implement proper corporate governance principles in the daily functioning of businesses. Whistle-blowing is designed as an additional mechanism for employees to report misconduct internally through a specific channel and supplements a business’s regular information and reporting channels, such as employee representatives, line management, quality-control personnel or internal auditors who are employed precisely to report such misconduct.

The WP29 has limited its Opinion 1/2006 on the application of EU data protection rules to internal whistle-blowing schemes to the fields of accounting, internal accounting controls, auditing matters, and the fight against bribery, banking and financial crime. The scope of corporate whistle-blower hotlines, however, does not need to be limited to any particular issues. In the Opinion, it is recommended that the business responsible for the whistle-blowing scheme should carefully assess whether it might be appropriate to limit the number of persons eligible for reporting alleged misconduct through the whistle-blowing scheme and whether it might be appropriate to limit the number of persons who may be reported through the scheme, in particular in the light of the seriousness of the alleged offences reported.

Under French law, some provisions protect whistle-blowers against any discrimination regarding their salary, professional evolution with regards to conflict of interest concerning a state representative, corruption (article L. 1132-3-3 of the French labour code), serious risk to the health, the environment or the safety of sanitary or cosmetic products, moral or sexual harassment (articles L. 1152-1 and further and article L. 1153-1 and further of the French labour code), discrimination (article L. 1132-3 of the French labour code), serious danger for his/her life or health, defective protection systems (article L. 4131-1 of the French labour code). No specific provision is dedicated to the protection of personal data.

Anonymous reporting is not prohibited under EU data protection law; however, it raises problems as regards the essential requirement that personal data should only be collected fairly. In Opinion 1/2006, the WP29 considered that only identified reports should be advertised in order to satisfy this requirement. Businesses should not encourage or advertise the fact that anonymous reports may be made through a whistle-blower scheme.

An individual who intends to report to a whistle-blowing system should be aware that he/she will not suffer due to his/her action. The whistle-blower, at the time of establishing the first contact with the scheme, should be informed that his/her identity will be kept confidential at all the stages of the process, and in particular will not be disclosed to third parties, such as the incriminated person or to the employee’s line management. If, despite this information, the person reporting to the scheme still wants to remain anonymous, the report will be accepted into the scheme. Whistle-blowers should be informed that their identity may need to be disclosed to the relevant people involved in any further investigation or subsequent judicial proceedings instigated as a result of any enquiry conducted by the whistle-blowing scheme.

Internal whistle-blowing schemes are generally established in pursuance of a concern to implement proper corporate governance principles in the daily functioning of businesses. Whistle-blowing is designed as an additional mechanism for employees to report misconduct internally through a specific channel and supplements a business’s regular information and reporting channels, such as employee representatives, line management, quality-control personnel or internal auditors who are employed precisely to report such misconduct.

The WP29 has limited its Opinion 1/2006 on the application of EU data protection rules to internal whistle-blowing schemes to the fields of accounting, internal accounting controls, auditing matters, and the fight against bribery, banking and financial crime. The scope of corporate whistle-blower hotlines, however, does not need to be limited to any particular issues. In the Opinion, it is recommended that the business responsible for the whistle-blowing scheme should carefully assess whether it might be appropriate to limit the number of persons eligible for reporting alleged misconduct through the whistle-blowing scheme and whether it might be appropriate to limit the number of persons who may be reported through the scheme, in particular in the light of the seriousness of the alleged offences reported.

Under French law, some provisions protect whistle-blowers against any discrimination regarding their salary, professional evolution with regards to conflict of interest concerning a state representative, corruption (article L. 1132-3-3 of the French labour code), serious risk to the health, the environment or the safety of sanitary or cosmetic products, moral or sexual harassment (articles L. 1152-1 and further and article L. 1153-1 and further of the French labour code), discrimination (article L. 1132-3 of the French labour code), serious danger for his/her life or health, defective protection systems (article L. 4131-1 of the French labour code). No specific provision is dedicated to the protection of personal data.

Anonymous reporting is not prohibited under EU data protection law; however, it raises problems as regards the essential requirement that personal data should only be collected fairly. In Opinion 1/2006, the WP29 considered that only identified reports should be advertised in order to satisfy this requirement. Businesses should not encourage or advertise the fact that anonymous reports may be made through a whistle-blower scheme.

An individual who intends to report to a whistle-blowing system should be aware that he/she will not suffer due to his/her action. The whistle-blower, at the time of establishing the first contact with the scheme, should be informed that his/her identity will be kept confidential at all the stages of the process, and in particular will not be disclosed to third parties, such as the incriminated person or to the employee’s line management. If, despite this information, the person reporting to the scheme still wants to remain anonymous, the report will be accepted into the scheme. Whistle-blowers should be informed that their identity may need to be disclosed to the relevant people involved in any further investigation or subsequent judicial proceedings instigated as a result of any enquiry conducted by the whistle-blowing scheme.
If the data protection authority is of the opinion that the CCTV monitoring would infringe the GDPR, it has to provide written advice to the controller within eight weeks of the request of a consultation and can use any of its wider advisory, investigative and corrective powers outlined in the GDPR.

13.2 Are there limits on the purposes for which CCTV data may be used?

A CCTV system shall not be used directly to watch employees, unless their work is critical (dealing with money, stock of high-value goods). A CCTV system shall not film break rooms, rooms dedicated to unions, and toilets. Films shall be erased after one month. Public notices shall be put on walls.

14 Employee Monitoring

14.1 What types of employee monitoring are permitted (if any), and in what circumstances?

Geolocation of vehicles driven by employees is possible, but with some prohibitions; this system is not allowed to collect information when the driver is outside his/her working time, or to check the movements of union representatives. Drivers shall be informed that a geolocation system is on the car. The driver may be able to deactivate the system outside his/her working time. Collected information may be kept for two months, one year or five years, depending on the purpose of the installation of this system.

Registration of phone calls is allowed for training or evaluation of employees. Employees may deactivate the registration system or be provided with phones not linked to a registration system. Conversations of union representatives cannot be registered. In most cases, registration of phone calls shall be erased after six months.

Control of access to offices and the review of working time is possible through the use of access cards to the company’s offices. This information may be kept for three months or five years.

The employer may control the use of computers, access to the internet and emails exchanged by its employees, unless the email was labelled “personal/private”.

14.2 Is consent or notice required? Describe how employees typically obtain consent or provide notice.

Employees shall be informed that their activity is subject to employee monitoring tools. Employees cannot oppose the use of such tools if the installation is necessary and corresponds to the legal limits which authorise the installation of such tools. However, employees shall not be “controlled” outside of their working time.

Only authorised persons may have access to information collected by way of the employee monitoring tools.

14.3 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?

Unions shall be consulted before the installation of employee monitoring tools (article L. 2323-47 and L. 2312-38 of the French labour code). Otherwise, the employer is subject to criminal sanctions.

15 Data Security and Data Breach

15.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?

Yes. Personal data must be processed in a way which ensures security and safeguards against unauthorised or unlawful processing, accidental loss, destruction and damage of the data.

Both controllers and processors must ensure they have appropriate technical and organisational measures to meet the requirements of the GDPR. Depending on the security risk, this may include the encryption of personal data, the ability to ensure the ongoing confidentiality, integrity and resilience of processing systems, an ability to restore access to data following a technical or physical incident and a process for regularly testing and evaluating the technical and organisational measures for ensuring the security of processing.

15.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

The controller is responsible for reporting a personal data breach without undue delay (and in any case within 72 hours of first becoming aware of the breach) to the relevant data protection authority, unless the breach is unlikely to result in a risk to the rights and freedoms of the data subject(s). A processor must notify any data breach to the controller without undue delay.

The notification must include the nature of the personal data breach, including the categories and number of data subjects concerned, the name and contact details of the Data Protection Officer or relevant point of contact, the likely consequences of the breach and the measures taken to address the breach including attempts to mitigate possible adverse effects.

Additionally, if the controller is an operator of essential services (“OES”) as defined in, it must notify security breaches to computer security incident response teams (“CSIRTs”) and other relevant bodies – in France, this is l’Agence nationale de la sécurité des systèmes d’information (“ANSSI”).

15.3 Is there a legal requirement to report data breaches to affected data subjects? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

Controllers have a legal requirement to communicate the breach to the data subject, without undue delay, if the breach is likely to result in a high risk to the rights and freedoms of the data subject.

The notification must include the name and contact details of the Data Protection Officer (or point of contact), the likely consequences of the breach and any measures taken to remedy or mitigate the breach.

The controller may be exempt from notifying the data subject if the risk of harm is remote (e.g., because the affected data is encrypted),
the controller has taken measures to minimise the risk of harm (e.g., suspending affected accounts) or the notification requires a disproportionate effort (e.g., a public notice of the breach).

15.4 What are the maximum penalties for data security breaches?

As first sanctions, the French control authority CNIL may pronounce the following measures: a reminder; and/or an injunction to comply with the regulation with an eventual penalty of up to €100,000 per day. In major cases, the CNIL may also pronounce a penalty up to €10 million or 4% of worldwide turnover. The maximum penalty is the higher of €20 million or 4% of worldwide turnover in the event of breaches sentenced by points 5 and 6 of article 83 of the GDPR.

16 Enforcement and Sanctions

16.1 Describe the enforcement powers of the data protection authority(ies).

<table>
<thead>
<tr>
<th>Investigatory Power</th>
<th>Civil/Administrative Sanction</th>
<th>Criminal Sanction</th>
</tr>
</thead>
<tbody>
<tr>
<td>Investigative Powers</td>
<td>The data protection authority has wide powers to order the controller and the processor to provide any information it requires for the performance of its tasks, to conduct investigations in the form of data protection audits, to carry out review on certificates issued pursuant to the GDPR, to notify the controller or processor of alleged infringement of the GDPR, to access all personal data and all information necessary for the performance of controllers’ or processors’ tasks and access to the premises of the data including any data processing equipment.</td>
<td>The CNIL may refer the case to the French public prosecutor, or a data subject may raise a criminal complaint and a French judge may impose a criminal sanction which may lead to up to five years’ imprisonment and a fine of up to €300,000 (for individuals) to €1.5 million (if a company is held liable). In addition, if a criminal procedure is begun, the criminal judge can decide to take into account the amount of the administrative fine to determine the amount of the criminal fine (article 6, 7° of the draft of the French law of 13 February 2018).</td>
</tr>
<tr>
<td>Corrective Powers</td>
<td>The data protection authority has a wide range ofpowers including to issue warnings or reprimands for non-compliance, to order the controller to disclose a personal data breach to the data subject, to impose a permanent or temporary ban on processing, to withdraw a certification and to impose an administrative fine (as below).</td>
<td>Not applicable.</td>
</tr>
<tr>
<td>Authorisation and Advisory Powers</td>
<td>The data protection authority has a wide range of powers to advise the controller, accredit certification bodies and to authorise certificates, contractual clauses, administrative arrangements and binding corporate rules as outlined in the GDPR.</td>
<td>Not applicable.</td>
</tr>
<tr>
<td>Imposition of administrative fines for infringements of specified GDPR provisions</td>
<td>The GDPR provides for administrative fines which can be €20 million or up to 4% of the business’ worldwide annual turnover of the preceding financial year.</td>
<td>Not applicable.</td>
</tr>
<tr>
<td>Non-compliance with a data protection authority</td>
<td>The GDPR provides for administrative fines which will be €20 million or up to 4% of the business’ worldwide annual turnover of the preceding financial year, whichever is higher.</td>
<td>Not applicable.</td>
</tr>
</tbody>
</table>

16.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?

The GDPR entitles the relevant data protection authority to impose a temporary or definitive limitation, including a ban on processing. The relevant French regulation provides that the French control authority CNIL may issue such temporary or final ban.

16.3 Describe the data protection authority’s approach to exercising those powers, with examples of recent cases.

Considering that the GDPR is a very new regulation, no cases exist on this matter. It is nevertheless interesting to note that the French authority CNIL may intervene before courts that deal with GDPR issues and express observations.

16.4 Does the data protection authority ever exercise its powers against businesses established in other jurisdictions? If so, how is this enforced?

The French control authority CNIL may collaborate with other EU control authorities in accordance with articles 60 to 67 of the GDPR.
17 E-discovery / Disclosure to Foreign Law Enforcement Agencies

17.1 How do businesses typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?

The disclosure of personal data within the scope of a foreign discovery is possible, but only to the extent that such requests comply with certain rules: the request for personal data has to be for a legitimate purpose and respect professional secrecy; the communication of personal data shall be proportionate to the purpose of the discovery; the keeping of the communicated personal data shall be limited to a fixed period; the claimant shall disclose security measures taken to manage personal data in order to protect the rights attached to personal data; and the transfer of personal data shall respect the rules relating to the transfer of personal data outside France/the EU.

17.2 What guidance has/have the data protection authority(ies) issued?

The WP29 issued a working document in 2009 (WP158), which inspired the work done by CNIL on 23 July 2009 relating to guidelines concerning discovery requested by US agencies (decision n°2009-474).

18 Trends and Developments

18.1 What enforcement trends have emerged during the previous 12 months? Describe any relevant case law.

A recent decision of CNIL on 8 January 2018 sentenced a major distributor to a €100,000 penalty: the distributor, acting as controller, delegated the management of personal data to a processor; further to a claim notified to the CNIL, it was discovered that non-authorised persons could consult the personal data. CNIL subsequently ruled that the distributor was liable for mismanagement by allowing its sub-contractor to act as a processor.

18.2 What “hot topics” are currently a focus for the data protection regulator?

In 2018 the CNIL published a report mentioning its focus for 2019:

- voice assistants such as Alexa, Siri or Google Assistant, which are continuously listening to private discussions, which may breach privacy and personal data regulation;
- cloud computing, which continues to develop (25% of businesses’ data, according to Independent Focus Group research), whereas it remains highly vulnerable to attacks and breaches;
- data exchanges between private and public entities, particularly in the context of “connected cities”; and
- political communication (for election campaigns, etc.), which requires the processing of highly sensitive information such as political opinions.
We provide businesses with full-service data protection and privacy advice across all industry sectors, enabling clients to focus their resources on other business needs.

Data privacy and protection is absolutely fundamental to all types of organisation due to the increasing threat of malicious hackers with the ability to leverage and monetise information.

Multi-national organisations face a web of complex and conflicting laws and regulations surrounding the collection, use, retention and disclosure of information. This requires careful attention to data privacy at every stage of the business cycle to avoid the negative publicity surrounding data breaches.

Our team brings together a wealth of experience across a range of sectors and industries to keep you on the cutting edge of developments in the industry. Our strong working relationships with the regulators and industry bodies enable us to resolve issues and provide practical commercial advice.

We advise a wide range of businesses including retailers, insurers, hospitals, information service providers, technology start-ups, financial institutions, educational institutions and governments across the world on the full range of data issues.

We provide businesses with full-service data protection and privacy advice across all industry sectors, enabling clients to focus their resources on other business needs.

Data privacy and protection is absolutely fundamental to all types of organisation due to the increasing threat of malicious hackers with the ability to leverage and monetise information.

Multi-national organisations face a web of complex and conflicting laws and regulations surrounding the collection, use, retention and disclosure of information. This requires careful attention to data privacy at every stage of the business cycle to avoid the negative publicity surrounding data breaches.

Our team brings together a wealth of experience across a range of sectors and industries to keep you on the cutting edge of developments in the industry. Our strong working relationships with the regulators and industry bodies enable us to resolve issues and provide practical commercial advice.

We advise a wide range of businesses including retailers, insurers, hospitals, information service providers, technology start-ups, financial institutions, educational institutions and governments across the world on the full range of data issues.

Benjamin practises litigation before civil, commercial, administrative and criminal courts. He acts for major companies, both domestic and international. He is interested in various fields such as transportation, insurance, banking and new areas such as data protection.

His is recognised by Who’s Who Legal and The Legal 500.

Jean-Michel is a Legal Director focusing on business, corporate, insurance and reinsurance law and drafting agreements requiring special care on the protection of personal data.

Having practised for over 20 years, Jean-Michel handles mergers and acquisitions, international agreements and commercial leases. His wide commercial practice encompasses both advice and litigation. Jean-Michel regularly advises on the establishment, structuring of new entities and on group restructurings, and has substantial experience in advising foreign companies on investing in the French market (from counselling to litigation) on business law and corporate law matters.

His insurance and reinsurance practice entails commercial drafting and reviewing general terms of insurance policies. He represents all parties in the distribution and management of insurance policies. Much of his work relates to cross-border business and regulatory aspects of the insurance sector. In addition, he advises insurers on European and French operations.
1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

Since 25 May 2018, the principal data protection legislation in the EU has been Regulation (EU) 2016/679 (the “General Data Protection Regulation” or “GDPR”). The GDPR repealed Directive 95/46/EC (the “Data Protection Directive”) and has led to increased (though not total) harmonisation of data protection law across the EU Member States.

In addition to the GDPR, Germany has enacted the Federal Data Protection Act of 30 June 2017 (Bundesdatenschutzgesetz – “BDSG”), which specifies the principles and provisions of the GDPR for Germany.

1.2 Is there any other general legislation that impacts data protection?

The Federal Telecommunications Act (Telekommunikationsgesetz – “TKG”) of 22 June 2004 (as amended by the Act of 29 November 2018) implements the requirements of Directive 2002/58/EC (as amended by Directive 2009/136/EC) (the “ePrivacy Directive”), which provides a specific set of privacy rules to harmonise the processing of personal data by the telecoms sector. In January 2017, the European Commission published a proposal for an ePrivacy regulation (the “ePrivacy Regulation”) that would harmonise the applicable rules across the EU. In September 2018, the Council of the European Union published proposed revisions to the draft. The ePrivacy Regulation is still a draft at this stage and it is unclear when it will be finalised.

1.3 Is there any sector-specific legislation that impacts data protection?

In Germany, statutory Federal laws as well as statutory State laws provide sector-specific provisions that directly or indirectly impact data protection. However, any German statutory law impacting data protection will be interpreted in accordance with the principles of the GDPR.

1.4 What authority(ies) are responsible for data protection?

The Federal States (Länder) have jurisdiction for the enforcement of data protection laws. Accordingly, 16 State authorities are responsible for data protection in the private sector. The Federal Data Protection Commissioner is responsible for data protection in the telecommunications sector.

2 Definitions

2.1 Please provide the key definitions used in the relevant legislation:

- **“Personal Data”** means any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

- **“Processing”** means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

- **“Controller”** means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

- **“Processor”** means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

- **“Data Subject”** means an individual who is the subject of the relevant personal data.

- **“Sensitive Personal Data”** are personal data, revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, data concerning health or sex life and sexual orientation, genetic data or biometric data.

- **“Data Breach”** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.
**3 Territorial Scope**

### 3.1 Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to those laws?

The GDPR applies to businesses that are established in any EU Member State, and that process personal data (either as a controller or processor, and regardless of whether or not the processing takes place in the EU) in the context of that establishment.

A business that is not established in any Member State, but is subject to the laws of a Member State by virtue of public international law is also subject to the GDPR.

The GDPR applies to businesses outside the EU if they (either as controller or processor) process the personal data of EU residents in relation to: (i) the offering of goods or services (whether or not in return for payment) to EU residents; or (ii) the monitoring of the behaviour of EU residents (to the extent that such behaviour takes place in the EU).

Further, the GDPR applies to businesses established outside the EU if they monitor the behaviour of EU residents (to the extent such behaviour takes place in the EU).

**4 Key Principles**

### 4.1 What are the key principles that apply to the processing of personal data?

- **Transparency**
  Personal data must be processed lawfully, fairly and in a transparent manner. Controllers must provide certain minimum information to data subjects regarding the collection and further processing of their personal data. Such information must be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

- **Lawful basis for processing**
  Processing of personal data is lawful only if, and to the extent that, it is permitted under EU data protection law. The GDPR provides an exhaustive list of legal bases on which personal data may be processed, of which the following are the most relevant for businesses: (i) prior, freely given, specific, informed and unambiguous consent of the data subject; (ii) contractual necessity (i.e., the processing is necessary for the performance of a contract to which the data subject is a party, or for the purposes of pre-contractual measures taken at the data subject’s request); (iii) compliance with legal obligations (i.e., the controller has a legal obligation, under the laws of the EU or an EU Member State, to perform the relevant processing); or (iv) legitimate interests (i.e., the processing is necessary for the purposes of legitimate interests pursued by the controller, except where the controller’s interests are overridden by the interests, fundamental rights or freedoms of the affected data subjects).

  Please note that businesses require stronger grounds to process sensitive personal data. The processing of sensitive personal data is only permitted under certain conditions, of which the most relevant for businesses are: (i) explicit consent of the affected data subject; (ii) the processing is necessary in the context of employment law; or (iii) the processing is necessary for the establishment, exercise or defence of legal claims.

- **Purpose limitation**
  Personal data may only be collected for specified, explicit and legitimate purposes and must not be further processed in a manner that is incompatible with those purposes. If a controller wishes to use the relevant personal data in a manner that is incompatible with the purposes for which they were initially collected, it must: (i) inform the data subject of such new processing; and (ii) must be able to rely on a lawful basis as set out above.

- **Data minimisation**
  Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which those data are processed. A business should only process the personal data that it actually needs to process in order to achieve its processing purposes.

- **Accuracy**
  Personal data must be accurate and, where necessary, kept up to date. A business must take every reasonable step to ensure that personal data that are inaccurate are either erased or rectified without delay.

- **Retention**
  Personal data must be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

- **Data security**
  Personal data must be processed in a manner that ensures appropriate security of those data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

- **Accountability**
  The controller is responsible for, and must be able to demonstrate, compliance with the data protection principles set out above.

**5 Individual Rights**

### 5.1 What are the key rights that individuals have in relation to the processing of their personal data?

- **Right of access to data/copies of data**
  A data subject has the right to obtain from a controller the following information in respect of the data subject’s personal data: (i) confirmation of whether, and where, the controller is processing the data subject’s personal data; (ii) information about the purposes of the processing; (iii) information about the categories of data being processed; (iv) information about the categories of recipients with whom the data may be shared; (v) information about the period for which the data will be stored (or the criteria used to be determined that period); (vi) information about the existence of the rights to erasure, to rectification, to restriction of processing and to object to processing; (vii) information about the existence of the right to complain to the relevant data protection authority; (viii) where the data were not collected from the data subject, information as to the source of the data; and (ix) information about the existence of, and an explanation of the logic involved in, any automated processing that has a significant effect on the data subject.

  Additionally, the data subject may request a copy of the personal data being processed.

- **Right to rectification of errors**
  Controllers must ensure that inaccurate or incomplete data are erased or rectified. Data subjects have the right to rectification of inaccurate personal data.
- **Right to deletion/right to be forgotten**
  Data subjects have the right to erasure of their personal data (the "right to be forgotten") if: (i) the data are no longer needed for their original purpose (and no new lawful purpose exists); (ii) the lawful basis for the processing is the data subject’s consent, the data subject withdraws that consent, and no other lawful ground exists; (iii) the data subject exercises the right to object, and the controller has no overriding grounds for continuing the processing; (iv) the data have been processed unlawfully; or (v) erasure is necessary for compliance with EU law or national data protection law.

- **Right to object to processing**
  Data subjects have the right to object, on grounds relating to their particular situation, to the processing of personal data where the basis for that processing is either public interest or legitimate interest of the controller. The controller must cease such processing unless it demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the relevant data subject or requires the data in order to establish, exercise or defend legal rights.

- **Right to restrict processing**
  Data subjects have the right to restrict the processing of personal data, which means that the data may only be held by the controller, and may only be used for limited purposes if: (i) the accuracy of the data is contested (and only for as long as it takes to verify that accuracy); (ii) the processing is unlawful and the data subject requests restriction (as opposed to exercising the right to erasure); (iii) the controller no longer needs the data for their original purpose, but the data are still required by the controller to establish, exercise or defend legal rights; or (iv) verification of overriding grounds is pending, in the context of an erasure request.

- **Right to data portability**
  Data subjects have a right to receive a copy of their personal data in a commonly used machine-readable format, and transfer their personal data from one controller to another or have the data transmitted directly between controllers.

- **Right to withdraw consent**
  A data subject has the right to withdraw their consent at any time. The withdrawal of consent does not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject must be informed of the right to withdraw consent. It must be as easy to withdraw consent as to give it.

- **Right to object to marketing**
  Data subjects have the right to object to the processing of personal data for the purpose of direct marketing, including profiling.

- **Right to complain to the relevant data protection authority(ies)**
  Data subjects have the right to lodge complaints concerning the processing of their personal data with the relevant State authority, if the data subjects live in Germany or the alleged infringement occurred in Germany.

- **Right to basic information**
  Data subjects have the right to be provided with information on the identity of the controller, the reasons for processing their personal data and other relevant information necessary to ensure the fair and transparent processing of personal data.

### 6 Registration Formalities and Prior Approval

#### 6.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?

No; in general, there is no legal obligation in Germany for a business to notify the data protection authority or any other governmental body in respect of its processing activities. Sector-specific obligations may apply in exceptional cases. For instance, processing of data relating to health insurance can require the notification of the competent supervisory authority.

#### 6.2 If such registration/notice is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?

In general, there is no registration or notification required for data processing in Germany. Exceptional specific notification requirements are subject to the sector-specific provisions.

#### 6.3 On what basis are registrations/notifications made (e.g., per legal entity, per processing purpose, per data category, per system or database)?

In general, there is no registration or notification required for data processing in Germany. Exceptional specific notification requirements are subject to the sector-specific provisions.

#### 6.4 Who must register with/notify the data protection authority (e.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation)?

In general, there is no registration or notification required for data processing in Germany. Exceptional specific notification requirements are subject to the sector-specific provisions.

#### 6.5 What information must be included in the registration/notification (e.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes)?

In general, there is no registration or notification required for data processing in Germany. Exceptional specific notification requirements are subject to the sector-specific provisions.

#### 6.6 What are the sanctions for failure to register/notify where required?

In general, there is no registration or notification required for data processing in Germany. Exceptional specific notification requirements are subject to the sector-specific provisions.
6.7 What is the fee per registration/notification (if applicable)?

In general, there is no registration or notification required for data processing in Germany. Exceptional specific notification requirements are subject to the sector-specific provisions.

6.8 How frequently must registrations/notifications be renewed (if applicable)?

In general, there is no registration or notification required for data processing in Germany. Exceptional specific notification requirements are subject to the sector-specific provisions.

6.9 Is any prior approval required from the data protection regulator?

In general, there is no registration or notification required for data processing in Germany. Exceptional specific notification requirements are subject to the sector-specific provisions.

6.10 Can the registration/notification be completed online?

In general, there is no registration or notification required for data processing in Germany. Exceptional specific notification requirements are subject to the sector-specific provisions.

6.11 Is there a publicly available list of completed registrations/notifications?

In general, there is no registration or notification required for data processing in Germany. Exceptional specific notification requirements are subject to the sector-specific provisions.

6.12 How long does a typical registration/notification process take?

In general, there is no registration or notification required for data processing in Germany. Exceptional specific notification requirements are subject to the sector-specific provisions.

7 Appointment of a Data Protection Officer

7.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.

The appointment of a Data Protection Officer for controllers or processors is only mandatory in some circumstances, including where there is: (i) large-scale regular and systematic monitoring of individuals; or (ii) large-scale processing of sensitive personal data.

According to Section 38 of the BDSG, in addition to Article 37 (1) (b) and (c) of Regulation (EU) 2016/679, the controller and processor shall designate a data protection officer if they constantly employ, as a rule, at least 10 persons dealing with the automated processing of personal data.

Where a business designates a Data Protection Officer voluntarily, the requirements of the GDPR apply as though the appointment were mandatory.

7.2 What are the sanctions for failing to appoint a Data Protection Officer where required?

In the circumstances where appointment of a Data Protection Officer is mandatory, failure to comply may result in the wide range of penalties available under the GDPR.

7.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect of his or her role as a Data Protection Officer?

The appointed Data Protection Officer should not be dismissed or penalised for performing their tasks and should report directly to the highest management level of the controller or processor.

The dismissal of an appointed Data Protection Officer is only permitted for good reason. After the activity as Data Protection Officer has ended, the Data Protection Officer may not be terminated for a year following the end of appointment, unless the employer has just cause to terminate without notice.

7.4 Can a business appoint a single Data Protection Officer to cover multiple entities?

A single Data Protection Officer is permitted by a group of undertakings provided that the Data Protection Officer is easily accessible from each establishment and is able to communicate in German language with German-based employees or competent authorities.

7.5 Please describe any specific qualifications for the Data Protection Officer required by law.

The Data Protection Officer should be appointed on the basis of professional qualities and should have an expert knowledge of data protection law and practices. While this is not strictly defined, it is clear that the level of expertise required will depend on the circumstances. For example, the involvement of large volumes of sensitive personal data will require a higher level of knowledge.

7.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?

A Data Protection Officer should be involved in all issues which relate to the protection of personal data. The GDPR outlines the minimum tasks required by the Data Protection Officer, which include: (i) informing the controller, processor and their relevant employees who process data of their obligations under the GDPR; (ii) monitoring compliance with the GDPR, national data protection legislation and internal policies in relation to the processing of personal data including internal audits; (iii) advising on data protection impact assessments and the training of staff; and (iv) co-operating with the data protection authority and acting as the authority’s primary contact point for issues related to data processing.

7.7 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?

Yes, the controller or processor must notify the data protection authority of the contact details of the designated Data Protection Officer.
7.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?

The Data Protection Officer does not necessarily need to be named in the public-facing privacy notice. However, the contact details of the Data Protection Officer must be notified to the data subject when personal data relating to that data subject are collected. As a matter of good practice, the Article 29 Working Party (the “WP29”) (now the European Data Protection Board (the “EDPB”)) recommended in its 2017 guidance on Data Protection Officers that both the data protection authority and employees should be notified of the name and contact details of the Data Protection Officer.

8 Appointment of Processors

8.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?

Yes. The business that appoints a processor to process personal data on its behalf, is required to enter into an agreement with the processor which sets out the subject matter for processing, the duration of processing, the nature and purpose of processing, the types of personal data and categories of data subjects and the obligations and rights of the controller (i.e., the business).

It is essential that the processor appointed by the business complies with the GDPR.

8.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?

The processor must be appointed under a binding agreement in writing. The contractual terms must stipulate that the processor: (i) only acts on the documented instructions of the controller; (ii) imposes confidentiality obligations on all employees; (iii) ensures the security of personal data that it processes; (iv) abides by the rules of regarding the appointment of sub-processors; (v) implements measures to assist the controller with guaranteeing the rights of data subjects; (vi) assists the controller in obtaining approval from the relevant data protection authority; (vii) either returns or destroys the personal data at the end of the relationship (except as required by EU or Member State law); and (viii) provides the controller with all information necessary to demonstrate compliance with the GDPR.

9 Marketing

9.1 Please describe any legislative restrictions on the sending of electronic direct marketing (e.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?).

Yes, prior consent is mandatory for the sending of electronic direct marketing (according to Article 13 of the ePrivacy Directive).

9.2 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.).

Telephone marketing requires prior consent according to local laws on unfair trade practices. Business-to-business telephone marketing consent may be assumed if specific circumstances may lead to the conclusion that the recipient may consent to such telephone activity in that specific case. Any objection against direct marketing activities of the recipient must be obeyed.

9.3 Do the restrictions noted above apply to marketing sent from other jurisdictions?

Yes, the requirements apply to any marketing activities targeting persons based in Germany regardless of the jurisdiction of the sender.

9.4 Is/are the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?

Yes, competent authorities follow complaints of consumers thoroughly and will enforce the rules on direct marketing very strictly.

9.5 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?

The purchase of addresses or any other contact detail data for marketing purposes is not lawful under the administrative practice of enforcement of the GDPR in Germany.

9.6 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?

The wide range of potential penalties and damages under the GDPR generally apply to marketing communications in breach of the GDPR. Additionally, such marketing activities will infringe the local laws on unfair trade practices, as well as the Act Against Unfair Competition (Gesetz gegen den unlauteren Wettbewerb – “UWG”).

10 Cookies

10.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).

Article 5 of the ePrivacy Directive has not yet been implemented in Germany, according to the Data Protection Authorities in Germany. Therefore, German authorities take the position that the GDPR has to be applied to cookies directly. Pursuant to the German Data Protection Authorities’ legal opinion, following the principle of Article 5 of the EU ePrivacy Directive, the storage of cookies (or other data) on an end user’s device requires prior consent (the applicable standard of consent is derived from the GDPR). For consent to be valid, it must be informed, specific, freely given and must constitute a real and unambiguous indication of the individual’s wishes. This does not apply if: (i) the cookie is for the sole purpose of carrying out the transmission of a communication over an electronic communications network; or (ii) the cookie is
strictly necessary to provide an “information society service” (e.g., a service over the internet) requested by the subscriber or user, which means that it must be essential to fulfil their request.

The EU Commission intends to pass a new ePrivacy Regulation that will replace the respective national legislation in the EU Member States. The ePrivacy Regulation is planned to come into force in 2019.

10.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?

Article 5 of the ePrivacy Directive has not yet been implemented in Germany, according to the Data Protection Authorities in Germany. The legal opinion of the German Data Protection Authorities does not distinguish between different types of cookies.

10.3 To date, has/have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?

No information on enforcement action related to cookies is publicly available yet. However, the Bavarian Data Protection Authority has conducted a test on cookie compliance and announced enforcement activities against non-compliance, for implementation in the near future.

10.4 What are the maximum penalties for breaches of applicable cookie restrictions?

The wide range of potential penalties and damages of the GDPR generally apply.

11 Restrictions on International Data Transfers

11.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.

Data transfers to other jurisdictions that are not within the European Economic Area (the “EEA”) can only take place if the transfer is to an “Adequate Jurisdiction” (as specified by the EU Commission), the business has implemented one of the required safeguards as specified by the GDPR, or one of the derogations specified in the GDPR applies to the relevant transfer. The EDPB Guidelines (2/2018) set out that a “layered approach” should be taken with respect to these transfer mechanisms. If the transfer is not to an Adequate Jurisdiction, the data exporter should first explore the possibility of implementing one of the safeguards provided for in the GDPR before relying on a derogation.

11.2 Please describe the mechanisms businesses typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).

When transferring personal data to a country other than an Adequate Jurisdiction, businesses must ensure that there are appropriate safeguards on the data transfer, as prescribed by the GDPR. The GDPR offers a number of ways to ensure compliance for international data transfers, of which one is consent of the relevant data subject. Other common options are the use of Standard Contractual Clauses or BCRs.

Businesses can adopt the Standard Contractual Clauses drafted by the EU Commission – these are available for transfers between controllers, and transfers between a controller (as exporter) and a processor (as importer). International data transfers may also take place on the basis of contracts agreed between the data exporter and data importer provided that they conform to the protections outlined in the GDPR, and they have prior approval by the relevant data protection authority.

International data transfers within a group of businesses can be safeguarded by the implementation of Binding Corporate Rules (“BCRs”). The BCRs will always need approval from the relevant data protection authority. Most importantly, the BCRs will need to include a mechanism to ensure they are legally binding and enforced by every member in the group of businesses. Among other things, the BCRs must set out the group structure of the businesses, the proposed data transfers and their purpose, the rights of data subjects, the mechanisms that will be implemented to ensure compliance with the GDPR and the relevant complainant procedures.

Transfer of personal data to the USA is also possible if the data importer has signed up to the EU-US Privacy Shield Framework, which was designed by the US Department of Commerce and the EU Commission to provide businesses in the EU and the US with a mechanism to comply with data protection requirement when transferring personal data from the EU to the US.

11.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.

It is likely that the international data transfer will require prior approval from the relevant data protection authority unless they have already established a GDPR-compliant mechanism as set out above for such transfers.

In any case, most of the safeguards outlined in the GDPR will need initial approval from the data protection authority, such as the establishment of BCRs.

12 Whistle-blower Hotlines

12.1 What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?

Internal whistle-blowing schemes are generally established in pursuance of a concern to implement proper corporate governance principles in the daily functioning of businesses. Whistle-blowing is designed as an additional mechanism for employees to report misconduct internally through a specific channel and supplements a business’ regular information and reporting channels, such as employee representatives, line management, quality-control personnel or internal auditors who are employed precisely to report such misconducts.

The WP29 has limited its Opinion 1/2006 on the implementation of EU data protection rules to internal whistle-blowing schemes to the
fields of accounting, internal accounting controls, auditing matters, fight against bribery, banking and financial crime. The scope of corporate whistle-blower hotlines, however, does not need to be limited to any particular issues. In the Opinion it is recommended that the business responsible for the whistle-blowing scheme should carefully assess whether it might be appropriate to limit the number of persons eligible for reporting alleged misconduct through the whistle-blowing scheme and whether it might be appropriate to limit the number of persons who may be reported through the scheme, in particular in the light of the seriousness of the alleged offences reported.

12.2 Is anonymous reporting prohibited, strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do businesses typically address this issue?

Anonymous reporting is not prohibited under EU data protection law; however, it raises problems as regards the essential requirement that personal data should only be collected fairly. In the past, the German Data Protection Authorities took the position that anonymous whistle-blowing should not be permissible. In Opinion 1/2006, the WP29 considered that only identified reports should be advertised in order to satisfy the above-mentioned requirement. Businesses should not encourage or advertise the fact that anonymous reports may be made through a whistle-blower scheme.

An individual who intends to report to a whistle-blowing system should be aware that he/she will not suffer due to his/her action. The whistle-blower, at the time of establishing the first contact with the scheme, should be informed that his/her identity will be kept confidential at all the stages of the process, and in particular will not be disclosed to third parties, such as the incriminated person or to the employee’s line management. If, despite this information, the person reporting to the scheme still wants to remain anonymous, the report will be accepted into the scheme. Whistle-blowers should be informed that their identity may need to be disclosed to the relevant people involved in any further investigation or subsequent judicial proceedings instigated as a result of any enquiry conducted by the whistle-blowing scheme.

13 CCTV

13.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?

A data protection impact assessment (“DPIA”) must be undertaken with assistance from the Data Protection Officer when there is a systematic monitoring of a publicly accessible area on a large scale. If the DPIA suggests that the processing would result in a high risk to the rights and freedoms of individuals prior to any action being taken by the controller, the controller must consult the data protection authority.

During the course of a consultation, the controller must provide information on the responsibilities of the controller and/or processors involved, the purpose of the intended processing, a copy of the DPIA, the safeguards provided by the GDPR to protect the rights and freedoms of data subjects and where applicable, the contact details of the Data Protection Officer.

If the data protection authority is of the opinion that the CCTV monitoring would infringe the GDPR, it has to provide written advice to the controller within eight weeks of the request of a consultation and can use any of its wider investigative, advisory and corrective powers outlined in the GDPR.

13.2 Are there limits on the purposes for which CCTV data may be used?

According to Section 4 of the BDSG, monitoring publicly accessible areas with optical-electronic devices (video surveillance) shall be permitted only as far as it is necessary: (i) for public bodies to perform their tasks; (ii) to exercise the right to determine who shall be allowed or denied access; or (iii) to safeguard legitimate interests for specifically defined purposes and if there is nothing to indicate legitimate overriding interests of the data subjects.

For video surveillance of: (a) large publicly accessible facilities, such as sport facilities, places of gathering and entertainment, shopping centres and car parks; or (b) vehicles and large publicly accessible facilities of public rail, ship or bus transport, protecting the lives, health and freedom of persons present shall be regarded as a very important interest, according to Sec. 4 of the BDSG.

14 Employee Monitoring

14.1 What types of employee monitoring are permitted (if any), and in what circumstances?

According to Sec. 26 para 1 of the BDSG, personal data of employees may be processed for the detection of criminal offences if actual evidence to be documented substantiates the suspicion that the data subject has committed a criminal offence in the employment relationship, the processing is necessary for the detection and the legitimate interest of the employee in the exclusion of the processing is not predominant; in particular, the nature and extent are not disproportionate with regard to the cause. This shall also apply to severe infringements of contractual duties from the employment relationship. Secret monitoring of employees’ performance by technical means is not permitted. This includes video monitoring. However, monitoring for the purpose of ensuring data security or for any relevant safety purposes can be permissible on the legitimate interest basis. Information requirements under the GDPR have to be met at all times.

Employees’ private communication in transit is subject to the secrecy of telecommunications according to Sec. 88 of TKG. Thus, monitoring of employees’ private communication in transit is prohibited. Any infringement of telecommunications secrecy can constitute a criminal offence under the German Criminal Code. Potential co-determination rights of existing works councils remain unaffected.

14.2 Is consent or notice required? Describe how employers typically obtain consent or provide notice.

Generally, for monitoring that is not covered by statutory justification (see question 14.1 above), consent would be required. However, according to Sec. 26 para 2 of the BDSG, where personal data of employees shall be processed on the basis of consent, the assessment of the voluntary nature of the consent must take into account, in particular, the employment dependence of the employee and the circumstances in which the consent was given. German authorities have been very reluctant in the past to consider consent in employment relationships as being given freely, due to the inherent
dependence of the employee on his/her employer. Nevertheless, voluntariness may exist, in particular, if a legal or economic advantage is obtained for the employee or if the employer and the employee pursue similar interests. Consent must be given in writing, unless another form is appropriate due to special circumstances. Further, the employer must inform the employee personally, in text form, of the purpose of the data processing and of his/her right of withdrawal pursuant to Article 7 para. 3 of the GDPR.

Notice is generally provided at the beginning of the employment relationship (e.g. as an information annex to the employment contract). It is also best practice to provide and update all general privacy-related information in an intranet resource. Particular information related to special data processing should be provided ad hoc in that particular processing context.

15.3 Is there a legal requirement to report data breaches to affected data subjects? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

Controllers have a legal requirement to communicate the breach to the data subject, without undue delay, if the breach is likely to result in a high risk to the rights and freedoms of the data subject. The notification must include the name and contact details of the Data Protection Officer (or point of contact), the likely consequences of the breach and any measures taken to remedy or mitigate the breach.

The controller may be exempt from notifying the data subject if the risk of harm is remote (e.g., because the affected data is encrypted), the controller has taken measures to minimise the risk of harm (e.g., suspending affected accounts) or the notification requires a disproportionate effort (e.g., a public notice of the breach).

15.4 What are the maximum penalties for data security breaches?

The maximum penalty is the higher of €20 million or 4% of worldwide turnover, provided that the data security breach is due to non-compliance of the controller with the requirements of the GDPR.

16 Enforcement and Sanctions

16.1 Describe the enforcement powers of the data protection authority(ies).

<table>
<thead>
<tr>
<th>Investigatory Power</th>
<th>Civil/Administrative Sanction</th>
<th>Criminal Sanction</th>
</tr>
</thead>
<tbody>
<tr>
<td>Investigative Powers</td>
<td>The data protection authority has wide powers to order the controller and the processor to provide any information it requires for the performance of its tasks, to conduct investigations in the form of data protection audits, to carry out review on certificates issued pursuant to the GDPR, to notify the controller or processor of alleged infringement of the GDPR, to access all personal data and all information necessary for the performance of controllers’ or processors’ tasks and access to the premises of the data including any data processing equipment.</td>
<td>N/A</td>
</tr>
<tr>
<td>Corrective Powers</td>
<td>The data protection authority has a wide range of powers including to issue warnings or reprimands for non-compliance, to order the controller to disclose a personal data breach to the data subject, to impose a permanent or temporary ban on processing, to withdraw a certification and to impose an administrative fine (as below).</td>
<td>N/A</td>
</tr>
<tr>
<td>Authorisation and Advisory Powers</td>
<td>The data protection authority has a wide range of powers to advise the controller, accredit certification bodies and to authorise certificates, contractual clauses, administrative arrangements and binding corporate rules as outlined in the GDPR.</td>
<td>N/A</td>
</tr>
</tbody>
</table>
Germany’s Data Protection Authorities (17 State authorities and 1 Federal authority) have exercised their powers against Facebook through its establishment in Ireland.

### 17 E-discovery / Disclosure to Foreign Law Enforcement Agencies

#### 17.1 How do businesses typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?

Any data transfer in response to a foreign e-discovery must be lawful and in compliance with the provisions on international data transfer of the GDPR. Businesses will, in each case, assess both the legal basis for such data transfer and the adequacy of the level of data protection of the recipient. Businesses will, in most cases, refer foreign authorities to the system of international enforcement treaties. Strict retention policies, in compliance with the principle of storage limitation, will help businesses to keep to a minimum the amount of data they hold which is subject to e-discovery or disclosure.

#### 17.2 What guidance has/have the data protection authority(ies) issued?

The Article 29 Data Protection Working Party has issued the Working Document 1/2009 on pre-trial discovery for cross border civil litigation (WP158, adopted 11 February 2009) for further guidance. Although the Article 29 Data Protection Working Party ceased to exist on 25 May 2018 and the European Data Protection Board did not formally adopt all documents of the Article 29 Data Protection Working Party, the Working Document 1/2009 will still have persuasive effect and remains an important resource for guidance.

### 18 Trends and Developments

#### 18.1 What enforcement trends have emerged during the previous 12 months? Describe any relevant case law.

After a phase of consultation and support for businesses in the implementation of the requirements of the GDPR, German authorities began to make use of their enforcement powers in the second half of the year. The focus of enforcement activities was on the handling of data subject complaints and the enforcement of data subject rights, including the right to be forgotten. Reported administrative fines mostly dealt with unlawful data access.

For recent sanction cases, please see question 16.3 above. The State authorities are currently working on uniform guidelines for the imposition of fines in Germany to ensure a coherent enforcement of the GDPR in Germany.

#### 18.2 What “hot topics” are currently a focus for the data protection regulator?

German Data Protection Authorities take the position that the ePrivacy Directive has not yet been properly implemented in German law. Thus, the requirements of the GDPR apply directly to the use of cookies, and any tracking-related cookies would require consent. In February 2019 the Bavarian authority conducted an audit of the websites of 40 companies in Bavaria regarding cybersecurity and tracking technologies, and found that no website complied with the applicable requirements of the GDPR.
In the light of the recent case law of the European Court of Justice (e.g. judgment of 5 June 2018, C-210/16), German State authorities are debating the concept of joint controllership; in particular, in the context of the use of Facebook fan pages. In April 2019 German State authorities took the position that Facebook fan pages cannot be used in compliance with the GDPR by German companies.

The Bavarian authority announced a review of the ability to delete data within enterprise resource planning (“ERP”) software systems for 2019. Companies are advised to implement appropriate deletion concepts in their organisations.

Data subject rights will remain in the focus of the State authorities.

Dr. Axel von Walter, CIPP/E, CIPM is a Partner at BEITEN BURKHARDT’s Munich office and a member of the management board of the firm. He advises his clients on all areas of data protection, cyber security and information law, as well as competition law. In addition to operational advice, Dr. von Walter has extensive experience in litigation, particularly injunctive relief.

After studying law at the University of Munich, he was admitted to the German Bar in 2004. He has been Partner at BEITEN BURKHARDT since 2011. Before joining BEITEN BURKHARDT, he had been working for other international law firms in the field of IP/IT, media and data protection law, among others, in London. His doctoral thesis was awarded the Faculty Award of the faculty of law of the University of Munich.

Dr. von Walter is a lecturer in media and information law at the faculty of law at the University of Munich, and he is CIPP/E and CIPM-certified under the IAPP certification scheme for privacy professionals. He is frequently listed in the leading law firm rankings as a recommended lawyer (including The Legal 500 and JUVE).
Chapter 17

Ghana

Addison Bright Sloane

Victoria Bright

1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

The principal data protection legislation is the Data Protection Act, 2012 (Act 843) (“DPA”).

1.2 Is there any other general legislation that impacts data protection?

The fundamental basis for Ghana’s data protection law is Article 18 (2) of Ghana’s Constitution which guarantees that:

‘No person shall be subjected to interference with the privacy of his home, property, correspondence or communication except in accordance with law and as may be necessary in a free and democratic society for public safety or the economic well-being of the country, for the protection of health or morals, for the prevention of disorder or crime or for the protection of the rights or freedoms of others.’

1.3 Is there any sector-specific legislation that impacts data protection?

The sector-specific legislation that impacts data protection is as follows:

- Electronic Communications Act of Ghana, 2008 (Act 775) as amended by the Electronic Communications (Amendment) Act (Act 786).
- Unsolicited Electronic Communications Code of Conduct.

1.4 What authority(ies) are responsible for data protection?

The Data Protection Commission (“DPC”) is the authority responsible for data protection.

2 Definitions

2.1 Please provide the key definitions used in the relevant legislation:

- “Personal Data”
  Data about an individual who can be identified from the compiled data or other information in the possession of, or likely to come into the possession of the data controller.

- “Processing”
  An operation or activity or set of operations by automatic or other means that concerns data or personal data, and the:
  (i) collection, organisation, adaptation or alteration of the information or data;
  (ii) retrieval, consultation or use of the information or data;
  (iii) disclosure of the information or data by transmission, dissemination or other means available; or
  (iv) alignment, combination, blocking, erasure or destruction of the information or data.

- “Controller”
  A person who either alone, jointly or in common with other persons or as a statutory duty, determines the purposes for and the manner in which personal data is processed or is to be processed.

- “Processor”
  Any person other than an employee of the data controller who processes personal data on behalf of a data controller.

- “Data Subject”
  An individual who is the subject of personal data.

- “Sensitive Personal Data”
  The DPA refers to “special personal data” which is defined as personal data consisting of information related to:
  (i) a child who is under parental control according to the law; or
  (ii) the religious or philosophical beliefs, ethnic or tribal origin, colour, race, trade union membership, political opinions, physical or mental health, mental condition, DNA, sexual life, criminal behaviour of the data subject or details of court proceedings relating to the individual.

- “Data Breach”
  “Data Breach” is not defined in the DPA. However, there is provision for unauthorised access or acquisition of data as specified in questions 15.2 and 15.3.
3 Territorial Scope

3.1 Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to those laws?

- A data controller who is not incorporated in Ghana shall register as an external company where the data controller uses an equipment or a data processor carrying on business in Ghana to process the data, or processes data which originates partly or wholly from Ghana.
- The DPA does not apply to data which originates externally from other jurisdictions and merely transits through Ghana.
- In respect of foreign data subjects, the DPA requires personal data to be processed in compliance with the data protection laws of the foreign data subject, where data originating from the data subject’s jurisdiction is sent to Ghana for processing.

4 Key Principles

4.1 What are the key principles that apply to the processing of personal data?

- Accountability
  The DPA requires a person who processes personal data to ensure that the data is processed without infringing the rights of the data subject.
- Lawfulness of processing
  Data must be processed in a lawful and reasonable manner.
- Specification of purpose
  Personal data can only be processed if the purpose for which it is to be processed is necessary, relevant, and not excessive. The data controller must take necessary steps to ensure that the data subject is aware of the purpose for which the data is collected.
- Compatibility of further processing with purpose of collection
  Where a data controller holds personal data collected in connection with a specific purpose, any further processing of that data must be compatible with the purpose for which the personal data was initially obtained.
- Quality of information
  A data controller who processes personal data must ensure that the data is complete, accurate, up to date and not misleading, having regard to the purpose for which that data is collected or processed.
- Openness
  The openness principle ensures that individuals know about, and can participate in enforcing their rights under the DPA.
- A data controller who intends to process personal data must register with the DPC. A data controller who intends to collect data must also ensure that the data subject is aware of the nature of data being collected, the persons responsible for the collection, the purpose of the collection as well as whether or not the supply of data is mandatory or discretionary, among other things.
- Where the data is collected from a third party, the DPA requires the data subject to be informed before the data is collected, or as soon as practicable afterwards.
- The DPA provides circumstances under which the notification requirement is exempt, including where it is necessary to avoid compromising law enforcement, protect national security, or where it relates to the preparation or conduct of legal proceedings.

- Data security safeguards
  (i) A data controller has a duty to prevent the loss of, damage to, or unauthorised destruction of personal data, and the unlawful access to or unauthorised processing of personal data. The data controller must therefore adopt appropriate, reasonable, technical, and organisational means to take necessary steps to ensure the security of personal data in its possession or control.
  (ii) The data controller is also required to take reasonable measures to identify and forestall any reasonably foreseeable risks, and ensure that any safeguards put in place are effectively implemented and updated continually.
  (iii) The data controller must observe generally accepted and industry specific best practices in securing data, and ensure that data processors comply with security measures.

- Data subject participation
  An individual who provides proof of his identity, may request a data controller to confirm if the data controller holds that individual’s personal data, describe the nature of the personal data held, including the identity of a third party who has or has previously had access to that data. The request must be made in a reasonable manner and format, within a reasonable time, after paying any prescribed fees and in a form that is generally understandable.
  Upon receipt of the request, the data controller must either comply with the request or provide the data subject with credible evidence in support of the data.

5 Individual Rights

5.1 What are the key rights that individuals have in relation to the processing of their personal data?

- Right of access to data/copies of data
  The data subject has a right to access his personal data.
- Right to rectification of errors
  A data subject may request a data controller to have personal data held about the data subject corrected.
- Right to deletion/right to be forgotten
  A data subject can also request a data controller to:
  (i) correct or delete personal data about the data subject that is held by or under the control of the data controller and which is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully; or
  (ii) destroy or delete a record of personal data about the data subject held by the data controller that the data controller no longer has the authorisation to retain.
6 Registration Formalities and Prior Approval

6.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?

It is mandatory for all those who process personal data to register with the DPC. The DPC maintains a register of data controllers known as the Data Protection Register.

6.2 If such registration/notice is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?

Registration is detailed and specific. Knowingly providing false information is an offence punishable by a fine or imprisonment.

6.3 On what basis are registrations/notifications made (e.g., per legal entity, per processing purpose, per data category, per system or database)?

Registrations/notifications are made per legal entity qualifying as a data controller under the DPA. Additionally, where a data controller intends to keep personal data for two or more purposes, the DPC shall make separate entries for each purpose in the Register.

6.4 Who must register with/notify the data protection authority (e.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation)?

Any entity which qualifies as a data controller. A data controller is a person who either alone, jointly with other persons, or in common with other persons, or as a statutory duty, determines the purposes and the manner in which personal data is processed or is to be processed.

A data controller who is not incorporated in Ghana shall register as an external company.

Registration is compulsory with respect to:
(i) any legal entity established in Ghana processing personal data in Ghana. This includes a body incorporated under the laws of Ghana, a partnership registered under the Registration of Business Names Act, 1962;
(ii) any foreign legal entity using equipment, or a data processor established in Ghana to process personal data;
(iii) any legal entity or person processing data originating partly or wholly from Ghana;
(iv) any person who is ordinarily resident in Ghana;
(v) an unincorporated joint venture or association operating in whole or in part in Ghana; and
(vi) an individual who does not fall within any of the above categories but maintains an office, branch or agency through which business activities are carried out in Ghana.

6.5 What information must be included in the registration/notice (e.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes)?

The following must be included:
.a. the business name and address of the applicant;
b. the name and address of the company’s representative where the company is an external company;
c. a description of the personal data to be processed and the category of persons whose personal data are to be collected;
d. an indication as to whether the applicant holds or is likely to hold special personal data;
7 Appointment of a Data Protection Officer

7.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.

The wording in the DPA suggests it is optional. In practice, this is not the case, as explained in question 7.2 below.

7.2 What are the sanctions for failing to appoint a Data Protection Officer where required?

There are no stipulated sanctions in Ghanaian law for failing to appoint a Data Protection Supervisor. However, the registration process cannot be completed without specifying the full details of the Data Supervisor.

7.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect of his or her role as a Data Protection Officer?

The DPA makes no reference to any sanctions against the Data Protection Supervisor. All disciplinary sanctions are directed at the Data Controller and the Data Processor.

7.4 Can a business appoint a single Data Protection Officer to cover multiple entities?

The DPA is silent on this.

7.5 Please describe any specific qualifications for the Data Protection Officer required by law.

The Data Protection Supervisor is required to be a certified and qualified Data Supervisor. The criteria for qualification are as follows:

(i) very good knowledge of and proven experience in data protection issues;
(ii) the ability to act with required independence;
(iii) a clear understanding of the effects of further advances in technology on data protection, and the ability to identify, anticipate and tackle these challenges effectively and efficiently;
(iv) excellent analytical and judgment skills, able to solve organisational and operational problems;
(v) capacity for decision-making, combined with a strong ability to provide policy guidance so as to meet new and unforeseen challenges in data protection; and
(vi) high-level management experience to manage teams of highly specialised staff.

7.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?

The Data Protection Supervisor’s primary responsibility is to supervise and monitor the data controller’s compliance with the DPA.

e. a description of the purpose for which the personal data is being or is to be processed;
f. a description of a recipient to whom the applicant intends to disclose the personal data;
g. the name or description of the country to which the applicant may transfer the personal data;
h. the class of persons or, where practicable, the names of persons whose personal data is held by the applicant;
i. a general description of measures to be taken to secure the data; and
j. any other information that the DPC may require.

6.6 What are the sanctions for failure to register/notify where required?

A data controller who fails to register with the DPC is liable on summary conviction to a fine of not more than 250 penalty units or a term of imprisonment of not more than two years, or to both.

Note: 1 penalty unit is equivalent to 12 Cedis (2.33 USD as at April 2019).

6.7 What is the fee per registration/notification (if applicable)?

The registration fee depends on the classification category of the data controller, as follows:

(i) Small Data Controllers – 100 Cedis.
(ii) Medium Data Controllers – 750 Cedis.
(iii) Large Data Controllers – 1,500 Cedis.

The type of classification is decided by the DPC.

Note: 1 USD is equivalent to 5.15 Cedis as at April 2019.

6.8 How frequently must registrations/notifications be renewed (if applicable)?

Registrations/notifications must be renewed every two years.

6.9 Is any prior approval required from the data protection regulator?

The DPC must approve an application before certification for registration can be issued.

6.10 Can the registration//notification be completed online?

All registration is completed online.

6.11 Is there a publicly available list of completed registrations/notifications?

The DPC makes the Register available for inspection by members of the public. They may obtain a duly certified manual or electronic copy of the particulars for a prescribed fee.

6.12 How long does a typical registration/notification process take?

The DPC aims to complete registration within a few days of receiving the application with all supporting documentation.
7.7 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?

Details of the data protection supervisor are required to be specified as part of the application process.

7.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?

There is no requirement for the Data Protection Supervisor to be named in any public-facing privacy notice.

8 Appointment of Processors

8.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?

The processing of personal data by a data processor for a data controller must be governed by a contract.

8.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?

The contract must be in writing and shall require the data processor to establish and maintain the confidentiality and security measures necessary to ensure the integrity of the personal data. Where the processor is not domiciled in Ghana, the data controller shall ensure that the processor complies with the relevant laws of Ghana.

9 Marketing

9.1 Please describe any legislative restrictions on the sending of electronic direct marketing (e.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?).

A data controller is prohibited from providing, using, obtaining, procuring or providing information related to a data subject for the purposes of direct marketing without the prior written consent of the data subject.

9.2 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.).

The prohibition described in question 9.1 applies to all forms of direct marketing, regardless of the mechanism used.

9.3 Do the restrictions noted above apply to marketing sent from other jurisdictions?

The DPA is silent on this.

9.4 Is/are the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?

The DPC is presently not active in the enforcement of such breaches.

9.5 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?

It is an offence to purchase the personal data or the information contained in the personal data of another person.

9.6 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?

The offender will be liable on summary conviction to a fine of not more than 250 penalty units or a term of imprisonment of not more than two years, or both.

10 Cookies

10.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).

The DPA does not specifically address the use of cookies. There is a general prohibition on the retention of the personal data of an individual beyond the period necessary to achieve the purpose for which the data was collected and processed, except where the retention of the record is (i) required or authorised by law, (ii) reasonably necessary for a lawful purpose, (iii) required by virtue of a contract between the parties to a contract, or (iv) the data subject consents to retention of the record.

10.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?

The restrictions exclude personal data retained for historical, statistical or research purposes. Such information must be adequately protected against access or use for unauthorised purposes.

10.3 To date, has/have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?

The Commission is yet to take any enforcement action against organisations in respect of violations of cookie restrictions. In the interim, it has deployed a taskforce to investigate issues of non-compliance with the rules in various organisations in Ghana.

10.4 What are the maximum penalties for breaches of applicable cookie restrictions?

A person who breaches a cookie restriction is liable on summary conviction to a fine of not more than 5000 penalty units, or a term of imprisonment of not more than 10 years, or both.
11 Restrictions on International Data Transfers

11.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.

There are no specific provisions in the DPA on the transfer of personal data. However, the sale, purchase, knowing or reckless disclosure of personal data or information is prohibited.

11.2 Please describe the mechanisms businesses typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).

The DPA is silent on this. However, logically the exceptions to the grant of consent by a data subject to the processing of his personal data as specified under the DPA may be equally applicable in the case of foreign transfers. Thus businesses may transfer personal data abroad with the prior consent of the data subject, or where the purpose for which the personal data is processed is necessary for the purpose of a contract to which the data subject is a party, or to protect a legitimate interest of the data subject, or the transfer is necessary for the proper performance of a statutory duty, or is necessary to pursue the legitimate interest of the data controller, or a third party to whom the data is supplied.

The individual may object to the processing of his personal data at any time.

11.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.

There is no law on the registration of data transfer to other jurisdictions. However, a data controller who obtains the consent of a data subject to transfer his personal data or otherwise falls within the exemptions in question 11.2 must register with the DPC.

12 Whistle-blower Hotlines

12.1 What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?

The Whistle-blower Act, 2006 (Act 720) requires that disclosure must be made to the employer. The requirement is to report an impropriety.

12.2 Is anonymous reporting prohibited, strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do businesses typically address this issue?

Under the Whistle-blower Act, 2006 (Act 720), a disclosure made by the whistle-blower must contain his/her full particulars. Anonymous reporting is strongly discouraged. Businesses address this through whistleblowing policies.

13 CCTV

13.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?

Data controllers who process personal data through the use of CCTV systems are required to be registered by the DPC. However, the DPA exempts CCTV systems installed for the purposes of the individual’s personal, family or household affairs.

13.2 Are there limits on the purposes for which CCTV data may be used?

Personal data collected through the use of CCTV shall be used only for a purpose which is specific, explicitly defined and lawful and is related to the functions or activities of that person. Any further processing of personal data must be for the same specific purposes. Use of personal data other than for a specific, explicitly defined and lawful purpose is proscribed. CCTV data may generally be used for crime prevention purposes and cannot be lawfully used to monitor sensitive areas like sanitation rooms and bedrooms.

14 Employee Monitoring

14.1 What types of employee monitoring are permitted (if any), and in what circumstances?

The use of specific and conspicuous monitoring devices and records which is necessary for the purpose of the performance of the employment contract, compliance with a legal obligation, protection of an employee or necessary for the legitimate interest of the employer or a third party may be permissible under the law. However, secret recordings of employees in the absence of reasonable suspicion of a crime, as well as monitoring in sensitive areas like sanitation and break rooms, constitute infractions of the employee’s right to privacy.

14.2 Is consent or notice required? Describe how employers typically obtain consent or provide notice.

An employer is required to notify and obtain the consent of the employee before processing his personal data. However, the employer does not require consent to process data where it relates to that employee’s employment, is authorised by law, protects the legitimate interest of the employee, is necessary for the performance of a statutory duty or is necessary to pursue the legitimate interest of the employer or a third party to whom the data is supplied. Employers typically obtain consent from employees by including consent clauses in their employment contracts.

14.3 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?

Employers are not required to notify trade unions when processing or monitoring employee data.
15 Data Security and Data Breach

15.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.).?

The DPC enjoins all persons who process personal data to ensure, among other things, that the personal data is secured and safeguarded. The DPC is also required to ensure compliance with the data protection principles by data controllers and data processors. The DPA is required to keep the data it receives confidential.

15.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

The DPC requires the data controller, or a third party who processes data under the data controller’s authority, to report to the DPC where there are reasonable grounds to believe that the personal data of an individual has been accessed or acquired by an unauthorised person. The notification shall be made as soon as reasonably practicable after the discovery of the unauthorised access or acquisition of the data. The notification shall provide sufficient information about such unauthorised access or acquisition of data.

15.3 Is there a legal requirement to report data breaches to affected data subjects? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

The data controller, or a third party who processes data under the authority of the data controller, must report to the data subject where there are reasonable grounds to believe that the personal data of an individual has been accessed or acquired by an unauthorised person. The notification shall be made as soon as reasonably practicable after the discovery of the unauthorised access or acquisition of the data. The notification shall provide sufficient information about the unauthorised access or acquisition of data so as to allow the individual to take protective measures against the breach. The data controller shall delay the notification to the individual where the security agencies or the DPC inform the data controller that the notification will impede a criminal investigation.

15.4 What are the maximum penalties for data security breaches?

There are various offences under the DPA. Each carries different penalties.

A person who, in compliance with an information notice, knowingly or recklessly makes a statement which is false in a material respect, commits an offence and is liable on summary conviction to a fine of not more than 150 penalty units or to a term of imprisonment of not more than one year, or to both.

A person shall not purchase the personal data or the information contained in the personal data of another person, knowingly obtain or knowingly or recklessly disclose the personal data or the information contained in the personal data of another person, or disclose or cause to be disclosed to another person the information contained in such personal data. A person who contravenes the foregoing provision commits an offence punishable on summary conviction by a fine of not more than 250 penalty units or to a term of imprisonment of not more than two years, or to both.

A person who sells or offers to sell personal data of another person commits an offence punishable on summary conviction by a fine of not more than 2,500 penalty units or to a term of imprisonment of not more than five years, or to both.

There is a general penalty where a person who commits an offence under the DPA in respect of which a penalty is not specified is liable on summary conviction to a fine of not more than 5,000 penalty units or a term of imprisonment of not more than 10 years, or both.

16 Enforcement and Sanctions

16.1 Describe the enforcement powers of the data protection authority(ies).

<table>
<thead>
<tr>
<th>Investigatory Power</th>
<th>Civil/Administrative Sanction</th>
<th>Criminal Sanction</th>
</tr>
</thead>
<tbody>
<tr>
<td>Investigation and determination in a fair manner, of complaints under the DPA.</td>
<td>Issuing enforcement notices, which may include orders directing a data controller to refrain from processing personal data of a description stated in the notice, correction, erasure or destruction to personal data.</td>
<td>Prosecuting offences under the DPA (with the Attorney General’s collaboration). The DPC has no power to apply criminal sanctions. This remains the sole domain of the courts.</td>
</tr>
</tbody>
</table>

16.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?

Where the DPC is satisfied that a data controller has contravened or is contravening any of the data protection principles, the commission shall serve the data controller with an enforcement notice, which may include an order directing the data controller to refrain from processing personal data of the description specified in the notice. No court order is required.

16.3 Describe the data protection authority's approach to exercising those powers, with examples of recent cases.

The DPC’s approach to enforcement is usually through an enforcement notice requesting a data controller to take or refrain from taking a particular action or step within a certain time period. Such actions may include banning the processing of personal data, correction, erasure or destruction of personal data. The commission has power to investigate and prosecute (on the authority of the Attorney General’s Department) offences under the Act.
16.4 Does the data protection authority ever exercise its powers against businesses established in other jurisdictions? If so, how is this enforced?

The DPC’s powers of enforcement do not extend to businesses established outside Ghana. The DPA enjoins the DPC to perform its data protection functions in a manner that is necessary to give effect to Ghana’s international obligations. The DPC maintains enforcement cooperation with other data protection regulators internationally to bridge the jurisdiction gap.

17 E-discovery / Disclosure to Foreign Law Enforcement Agencies

17.1 How do businesses typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?

Typically, Ghanaian businesses are likely to decline requests from foreign law enforcement agencies for disclosure of personal data as they are not under any legal obligation to disclose the same. Foreign law enforcement agencies may have to work through international processes, such as treaties for mutual legal assistance or police-to-police cooperation agreements to access such data.

17.2 What guidance has/have the data protection authority(ies) issued?

The DPC has issued no specific guidelines on how to respond to requests for disclosure from foreign law enforcement agencies.

18 Trends and Developments

18.1 What enforcement trends have emerged during the previous 12 months? Describe any relevant case law.

The issuance of enforcement and information notices has emerged as the preponderant enforcement regime adopted by the DPC. There is generally a dearth of reported case law on data protection, as the subject is relatively young and still evolving in Ghana.

18.2 What “hot topics” are currently a focus for the data protection regulator?

Ensuring that data controllers, especially governmental agencies, are registered and their processing activities comply with the data protection principles, is the DPC’s primary focus. Additionally, the DPC is developing guidelines for the collection, use and storage of data by organisations in critical sectors such as health, security and education. Regarding enforcement, the DPC is deliberately refraining from taking punitive measures while educating Ghanaians on data protection issues. Presently, Ghanaians do not have much understanding of the DPA. The DPC has said it intends to publish the names of compliant companies in future to encourage registration and compliance.
Chapter 18

Hong Kong

Ashurst Hong Kong

1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

Hong Kong’s principal data protection legislation is the **Personal Data (Privacy) Ordinance (Cap. 486)** (the “**PDPO**”).

The PDPO came into force in 1996, and was one of Asia’s earliest comprehensive data privacy legislation. The PDPO is based on the Organisation for Economic Co-operation and Development’s **Guidelines on the Protection of Privacy and Transborder Flows of Personal Data**, which in turn was a foundation for Europe’s **Data Protection Directive EC95/46**. The PDPO was last amended in 2012, primarily in relation to direct marketing-related obligations. All clause references in this chapter are to the PDPO, unless otherwise expressly specified.

1.2 Is there any other general legislation that impacts data protection?

Except for the PDPO, there is no general data protection legislation.

1.3 Is there any sector-specific legislation that impacts data protection?

While there is no sector-specific data protection legislation:

- the Office of the Privacy Commissioner for Personal Data (“**PCPD**”) has issued various Guidance and codes of practice on how the PDPO applies in various contexts. While these documents are not the law per se, they represent the Privacy Commissioner for Personal Data’s (the “**Commissioner**”) views on PDPO compliance, and failure to comply with them will weigh unfavourably against the relevant data user in any case before the Commissioner;

- various regulators and industry associations have issued guidelines and codes of practice that may affect how data protection is addressed in those industries. For example, the Hong Kong Monetary Authority (the “**HKMA**”) has issued a **Circular on Customer Data Protection and a Supervisory Policy Manual on Risk Management of E-banking**, and the HKMA, Securities and Futures Commission (the “**SFC**”) and the Insurance Authority have all published guidelines on outsourcing – these documents contain provisions that are relevant to data protection; and

- there are various pieces of legislation that impact data protection-related areas. For example, a number of statutes allow government bodies to access or compel disclosure of personal data:
  - Section 44 allows the Commissioner to require the furnishing of information or documentation relevant to an investigation.
  - The **Interception of Communications and Surveillance Ordinance (Cap. 589)** enables law enforcement authorities to intercept communications and carry out covert surveillance subject to certain requirements.
  - Section 52 of the **Inland Revenue Ordinance (Cap. 112)** enables the Inland Revenue Department to require an employer to furnish information on an employee.
  - Various ordinances give public authorities/regulators the power to compel disclosure of information in relation to financial crimes – e.g. the **Anti-Money Laundering and Counter-Terrorist Financing (Financial Institutions) Ordinance (Cap. 615)**.

1.4 What authority(ies) are responsible for data protection?

The PCPD was established by the PDPO, and is an independent statutory body that enforces the PDPO. This Office is headed by the Commissioner. The current Commissioner is Mr. Stephen Wong Kai-Yi, appointed on 4 August 2015. The Commissioner noted in February 2019 that the PCPD had a total of 69 staff members.

2 Definitions

2.1 Please provide the key definitions used in the relevant legislation:

Unless otherwise specified, the following definitions are from the PDPO.

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition under the PDPO (if applicable)</th>
</tr>
</thead>
<tbody>
<tr>
<td>“Personal Data”</td>
<td>(a) relating directly or indirectly to a living individual;</td>
</tr>
<tr>
<td></td>
<td>(b) from which it is practicable for the identity of the individual to be directly or indirectly ascertained; and</td>
</tr>
<tr>
<td></td>
<td>(c) in a form in which access to or processing of the data is practicable.</td>
</tr>
</tbody>
</table>
In relation to personal data, includes amending, augmenting, deleting or rearranging the data, whether by automated means or otherwise.

“Controller” is the equivalent term for data controller under the PDPO. “Data User” in relation to personal data means a person who, either alone or jointly or in common with other persons, controls the collection, holding, processing or use of the data.

“Data Processor” means a person who: (a) processes personal data on behalf of another person; and (b) does not process the data for any of the person’s own purposes.

Note that PDPO obligations are on the data user, including in relation to ensuring that any engaged data processors also comply with relevant PDPO provisions.

In relation to personal data, means the individual who is the subject of the data.

This is not applicable in our jurisdiction.

This is not applicable in our jurisdiction.

This is not applicable in our jurisdiction.

“Data Breach” is not defined under the PDPO.

The PDPO is based on the following six Data Protection Principles (“DPP”) as set out in the PDPO:

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition under the PDPO (if applicable)</th>
</tr>
</thead>
<tbody>
<tr>
<td>“Processing”</td>
<td>In relation to personal data, includes amending, augmenting, deleting or rearranging the data, whether by automated means or otherwise.</td>
</tr>
<tr>
<td>“Controller”</td>
<td>“Data User” is the equivalent term for data controller under the PDPO. “Data User” in relation to personal data means a person who, either alone or jointly or in common with other persons, controls the collection, holding, processing or use of the data.</td>
</tr>
<tr>
<td>“Processor”</td>
<td>“Data Processor” means a person who: (a) processes personal data on behalf of another person; and (b) does not process the data for any of the person’s own purposes. Note that PDPO obligations are on the data user, including in relation to ensuring that any engaged data processors also comply with relevant PDPO provisions.</td>
</tr>
<tr>
<td>“Data Subject”</td>
<td>In relation to personal data, means the individual who is the subject of the data.</td>
</tr>
<tr>
<td>Sensitive Personal Data</td>
<td>This is not applicable in our jurisdiction. “Sensitive Personal Data” is not defined under the PDPO.</td>
</tr>
<tr>
<td>“Data Breach”</td>
<td>This is not applicable in our jurisdiction. “Data Breach” is not defined under the PDPO.</td>
</tr>
</tbody>
</table>

### Other key definitions under the PDPO

- **Data** means any representation of information (including an expression of opinion) in any document, and includes a personal identifier.
- **Document** includes, in addition to a document in writing: (a) a disc, tape or other device in which data other than visual images are embodied so as to be capable, with or without the aid of some other equipment, of being reproduced from the disc, tape or other device; and (b) a film, tape or other device in which visual images are embodied so as to be capable, with or without the aid of some other equipment, of being reproduced from the film, tape or other device.

**Direct marketing** means: (a) the offering, or advertising of the availability, of goods, facilities or services; or (b) the solicitation of donations or contributions for charitable, cultural, philanthropic, recreational, political or other purposes, through direct marketing means.

**Direct marketing means** means: (a) sending information or goods, addressed to specific persons by name, by mail, fax, electronic mail or other means of communication; or (b) making telephone calls to specific persons.

**Personal identifier** means an identifier: (a) that is assigned to an individual by a data user for the purpose of the operations of the user; and (b) that uniquely identifies that individual in relation to the data user, but does not include an individual’s name used to identify that individual.

### 3 Territorial Scope

#### 3.1 Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to those laws?

The PDPO does not confer extra-territorial application, and does not extend to bind any act committed by a foreign party in foreign territory.

Under section 39(1)(d), the Commissioner may terminate or refuse to carry out an investigation if the relevant complaint does not satisfy any of the following conditions:

- either:
  - the complainant was resident in Hong Kong at the time that the relevant act or practice was done or engaged in; or
  - the data user was able to control, in or from Hong Kong, the collection, holding, processing or use of the personal data at the relevant time;
- the complainant was in Hong Kong at the relevant time; or
- the act or practice that is subject to the complaint may (in the Commissioner’s opinion) prejudice the enforcement of any right, or the exercise of any privilege, acquired or accrued in Hong Kong by the complainant.

The above is consistent with the Commissioner’s public comments in relation to this topic.

### 4 Key Principles

#### 4.1 What are the key principles that apply to the processing of personal data?

The PDPO is based on the following six Data Protection Principles ("DPP") as set out in the PDPO:

<table>
<thead>
<tr>
<th>DPP</th>
<th>Content</th>
</tr>
</thead>
<tbody>
<tr>
<td>DPP1 – Data Collection Principle</td>
<td>Personal data must be collected in a lawful and fair way, for a purpose directly related to a function/activity of the data user. Data subjects must be notified of the purpose and the classes of persons to whom the data may be transferred. Data collected should be necessary but not excessive.</td>
</tr>
<tr>
<td>DPP2 – Accuracy and Retention Principle</td>
<td>Practicable steps shall be taken to ensure personal data is accurate and not kept longer than is necessary to fulfil the purpose for which it is used.</td>
</tr>
<tr>
<td>DPP3 – Data Use Principle</td>
<td>Personal data must be used for the purpose for which the data is collected or for a directly related purpose, unless voluntary and explicit consent with a new purpose is obtained from the data subject.</td>
</tr>
<tr>
<td>DPP4 – Data Security Principle</td>
<td>A data user needs to take practicable steps to safeguard personal data from unauthorised or accidental access, processing, erasure, loss or use.</td>
</tr>
<tr>
<td>DPP5 – Openness Principle</td>
<td>A data user must take practicable steps to make personal data policies and practices known to the public regarding the types of personal data it holds and how the data is used.</td>
</tr>
<tr>
<td>DPP6 – Data Access and Correction Principle</td>
<td>A data subject must be given access to his/her personal data and allowed to make corrections if it is inaccurate.</td>
</tr>
</tbody>
</table>
The below sets out how key data protection principles are addressed under the PDPO:

<table>
<thead>
<tr>
<th>Principle</th>
<th>How it is addressed in the PDPO</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transparency</td>
<td>Under DPP5, a data user must publicly disclose its policies and practices in relation to personal data, including the types of personal data held by the data user and the main purposes for which personal data is used.</td>
</tr>
<tr>
<td>Lawful basis for processing</td>
<td>Under DPP3, except with the express and voluntary consent of the data subject, personal data may only be used for the original purpose for which it was collected or a directly related purpose.</td>
</tr>
</tbody>
</table>
| Purpose limitation         | DPP1 sets out that in relation to personal data collection:  
                                ■ Personal data must be collected for a lawful purpose that is directly related to a function or activity of the data user.  
                                ■ Such collection must be necessary for or directly related to that purpose and not excessive in relation to that purpose.  
                                ■ Personal data should be collected by lawful and fair means.  
                                ■ A data user must provide certain information to the data subject when collecting the data subject’s personal data (see “Individual Rights” below). |
| Proportionality            | See DPP1 above.                                                                                |
| Data minimisation          | See DPP1 above.                                                                                |
| Retention                  | Under DPP2, data users must take all practicable steps to ensure that:  
                                ■ the personal data retained are accurate;  
                                ■ the personal data are not retained for any longer than is necessary for the lawful purpose for which the data were collected; and  
                                ■ when personal data are corrected that those corrections be provided to data users who were previously supplied the inaccurate data.  
                                If there are reasonable grounds for believing that personal data are inaccurate, data users should stop using the data. |
| Security                   | See DPP4 above.                                                                                |
| Data access and correction | A data subject has the right to ask a data user whether or not the data user holds any of his or her personal data, and to request a copy of such personal data held by that user. See also DPP6 above. |

The PDPO sets out certain exemptions in relation to particular types/uses of personal data:

<table>
<thead>
<tr>
<th>Exemption</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exemptions from PDPO</td>
<td>If personal data are in any interception or surveillance product, or documents in relation to prescribed authorisation or device retrieval warrant governed by the Interception of Communications and Surveillance Ordinance.</td>
</tr>
<tr>
<td>Exemptions from all DPP, Parts 4 and 5 and sections 36 and 38(b)</td>
<td>If personal data are held for performing judicial functions or domestic or recreational purposes.</td>
</tr>
</tbody>
</table>
| Exemption from DPP3        | If personal data are required in legal proceedings or relate to:  
                                ■ the identity or location of a data subject and the applications of DPP3 would likely cause serious harm to an individual’s health; or  
                                ■ care and guardianship of minors. |

Exemptions from DPP6 and section 18(1)(b)  
If personal data:  
■ relate to employment decisions or certain incomplete decision-making processes;  
■ are held by the government to safeguard security, defence or international relations of Hong Kong;  
■ relate to criminal proceedings, misconduct or malpractice;  
■ are held for tax purposes;  
■ are held for discharging functions of a financial regulator; or  
■ relate to legal professional privilege claims.  

Exemptions from DPP3, DPP6 and section 18(1)(b)  
If personal data relate to health of any individual or are used by the government to safeguard the security, defence or international relations of Hong Kong.

5 Individual Rights

5.1 What are the key rights that individuals have in relation to the processing of their personal data?

<table>
<thead>
<tr>
<th>Key right</th>
<th>Details</th>
</tr>
</thead>
</table>
| Right of access to data/copies of data         | Under DPP6, data subjects are entitled to:  
                                ■ ascertain whether a data user holds any of their personal data (paragraph 6(a) of Schedule 1);  
                                ■ request access to their personal data (paragraph 6(b) of Schedule 1); and  
                                ■ request correction of any inaccuracies in their personal data (paragraph 6(e) of Schedule 1).  
                                Data access requests can be made by completing the prescribed form (from the Commissioner) and submitting it to the data user.  
                                There is no prescribed form for requesting corrections to personal data – such requests may be made in writing.  
                                A data user must respond to data access and correction requests within 40 days (sections 19(1) and 23(1)) or notify the data subject of reasons why the data user is unable to process the request within the prescribed time period. |
| Right to rectification of errors              | See “right of access to data” above.                                                                                                   |
| Right to deletion/right to be forgotten       | There is no general right to deletion or to be forgotten.                                                                           |
| Right to object to processing                 | There is no general right to object to processing.                                                                                 |
| Right to restrict processing                  | There is no general right to restrict processing.                                                                                  |
| Right to data portability                     | There is no general right to data portability.                                                                                       |
| Exemption                                      | Details                                                                                                                                 |
| Exemptions from all DPP, Parts 4 and 5 and sections 36 and 38(b) | If personal data are held for performing judicial functions or domestic or recreational purposes.                                       |

When making a data access request, data subjects may request a copy of the relevant data in a specified form. The data user may provide the data in that specified form, or if it would not be reasonably practicable to do so, the data user may provide the data in another form.
### 6 Registration Formalities and Prior Approval

#### 6.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?

There is no such obligation under the PDPO. There may be sector-specific requirements that are relevant to the handling or protection of personal data in those sectors. For example, the HKMA’s Supervisory Policy Manual (http://www.hkma.gov.hk/eng/key-functions/banking-stability/supervisory-policy-manual.shtml) contains guidelines in relation to outsourcing and technology risk management that apply to financial institutions who are regulated by the HKMA and which may have an impact on such organisation’s processing activities.

#### 6.2 If such registration/notification is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?

This is not applicable in our jurisdiction.

#### 6.3 On what basis are registrations/notifications made (e.g., per legal entity, per processing purpose, per data category, per system or database)?

This is not applicable in our jurisdiction.

#### 6.4 Who must register with/notify the data protection authority (e.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation)?

This is not applicable in our jurisdiction.

#### 6.5 What information must be included in the registration/notification (e.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes)?

This is not applicable in our jurisdiction.

#### 6.6 What are the sanctions for failure to register/notify where required?

This is not applicable in our jurisdiction.

#### 6.7 What is the fee per registration/notification (if applicable)?

This is not applicable in our jurisdiction.

#### 6.8 How frequently must registrations/notifications be renewed (if applicable)?

This is not applicable in our jurisdiction.

#### 6.9 Is any prior approval required from the data protection regulator?

This is not applicable in our jurisdiction.

#### 6.10 Can the registration/notification be completed online?

This is not applicable in our jurisdiction.

#### 6.11 Is there a publicly available list of completed registrations/notifications?

This is not applicable in our jurisdiction.

#### 6.12 How long does a typical registration/notification process take?

This is not applicable in our jurisdiction.
7 Appointment of a Data Protection Officer

7.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.

The appointment of a Data Protection Officer is optional in Hong Kong. However, the Commissioner has published Guidance (https://www.pcpd.org.hk/files/PMP_guide_e.pdf) that encourages organisations to appoint a Data Protection Officer.

7.2 What are the sanctions for failing to appoint a Data Protection Officer where required?

This is not applicable in our jurisdiction.

7.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect to his or her role as a Data Protection Officer?

This is not applicable in our jurisdiction.

7.4 Can a business appoint a single Data Protection Officer to cover multiple entities?

This is not applicable in our jurisdiction.

7.5 Please describe any specific qualifications for the Data Protection Officer required by law.

This is not applicable in our jurisdiction.

7.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?

This is not applicable in our jurisdiction.

7.7 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?

This is not applicable in our jurisdiction.

7.8 Must the Data Protection Officer be named in a publicly-facing privacy notice or equivalent document?

This is not applicable in our jurisdiction.

8 Appointment of Processors

8.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?

Under the PDPO, if a data user engages a data processor (whether within or outside of Hong Kong) to process personal data on the data user’s behalf, the data user must adopt contractual or other means to prevent:

- any personal data transferred to the data processor from being kept longer than is necessary for processing of the data (DPP(3)); and
- any unauthorised or accidental access, processing, erasure, loss or use of the data transferred to the data processor for processing (DPP(4)).

A data user remains liable for its agent’s or contractor’s breach. Note that the PDPO does not:

- require a data user to first obtain a data subject’s consent to transfer personal data before transferring to the data processor. In practice, data users will usually notify data subjects about such practice; and
- distinguish between related and unrelated entities.

The Commissioner has issued Guidance in relation to data users outsourcing processing of personal data (https://www.pcpd.org.hk/english/publications/files/dataprocessors_e.pdf) and engaging cloud computing service providers (https://www.pcpd.org.hk/english/resources_centre/publications/files/IL_cloud_e.pdf) – including in relation to the type of contractual means (whether entire agreement or additional clauses) that data users should consider entering into with data processors.

8.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?

See above.

9 Marketing

9.1 Please describe any legislative restrictions on the sending of electronic direct marketing. (E.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?)

The PDPO has strict requirements in relation to direct marketing. Under the PDPO, “direct marketing” is defined as the offering, or advertising of the availability, of goods, facilities or services or the solicitation of donations or contributions for charitable, cultural, philanthropic, recreational, political or other purposes, through direct marketing means. Note that direct marketing does not include communications that are not directed to a specific individual by name.

A data user must inform a data subject of the data user’s intention to use the personal data in direct marketing, prior to such use. Specifically, a data user is required to inform data subjects of:

- its intention to use their personal data for direct marketing and that it can only do so with the data subject’s consent;
- the types of personal data will be used for direct marketing;
- the classes of goods, facilities or services offered, or the purposes for which any donation or contribution is solicited; and
- the response channel through which the data subject may communicate the data subject’s consent to the intended use.

The above information must be communicated to the data subject in a manner that is easily understandable and if in written form, easily readable. General descriptions of the types of goods offered or the
purposes of solicitation are not acceptable. In practice, one of the key issues in complying with direct marketing obligations is that the notification to data subjects must be sufficiently detailed with reference to the above points – general references to “certain products and services” are not sufficient to meet these requirements.

A data user must obtain consent of the data subject to the proposed direct marketing. As set out in the Commissioner’s New Guidance on Direct Marketing (https://www.pcpd.org.hk/english/publications/files/GN_DM_e.pdf), consent for direct marketing purposes includes an “indication of no objection” to the proposed use or provision. The “opt out” standard under the PDPO requires that data subjects explicitly indicate that their choice to opt out, for example, by signing and returning a form to the data user without checking the “opt out” box. Silence does not constitute consent.

If the data subject gives consent orally, the data user must send a written confirmation to the data subject within 14 days confirming the date of receipt of the consent and the scope of the consent obtained. When the data user uses the personal data in direct marketing for the first time, it must notify the data subject of its right to request the data user to stop using the personal data in direct marketing.

9.2 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.).

Under the Unsolicited Electronic Messages Ordinance (Cap. 591), the Hong Kong Communications Authority established Do-not-call Registers to protect the public from receiving unsolicited commercial electronic messages sent to their telephone or fax numbers. There are do-not-call registers for fax, short messages and pre-recorded telephone messages.

In April 2019, the Hong Kong Commerce and Economic Development Bureau (“CEDB”) set out its proposal to amend the Unsolicited Electronic Messages Ordinance (“UEMO”). The proposal focuses on direct person-to-person telemarketing calls that have “Hong Kong links” (i.e. originating in, an organisation conducting business in, or telecommunication devices being used that are located in, Hong Kong) – including extending the existing do-not-call register to cover such calls, and imposing fines and imprisonment on breaches of such law. The Hong Kong government has stated that this proposal is mainly aimed at reducing nuisance caused to members of the public, but they are also hoping to strike a balance as they do not want to obstruct business operations.

Specifically, under such proposal:

- If a subject has requested to be unsubscribed from such calls, telemarketers will have to stop dialling the relevant number within 10 working days, and record the request for at least three years.

- Telemarketers will need to provide accurate information, including who they are representing or the authorising organisation for the call, and their caller ID.

- There is a maximum penalty of HKD1,000,000 and five years’ imprisonment for a telemarketer who uses telephone number harvesting software and makes calls using automated means.

- An enforcement notice may be issued if the authority considers that a contravention has taken place (and may continue or be repeated), and require the relevant telemarketer to take remedial actions. If a telemarketer breaches that enforcement notice, they will face a maximum fine of HKD100,000 (for the first conviction) or HKD500,000 (for subsequent convictions).

We note that the above is a proposal, and no timeframe for passing or implementing such amendments has been set.

9.3 Do the restrictions noted above apply to marketing sent from other jurisdictions?

See question 3.1.

9.4 Is/are the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?

The direct marketing restrictions in the PDPO have been actively monitored and enforced by the Commissioner.

The Commissioner will, from time to time, make public announcements on its website in relation to its enforcement of the direct marketing restrictions. Such enforcement actions have resulted in enforcement notices (as referenced above) or in monetary penalties via Hong Kong courts.

The Commissioner has previously commented (in January 2018) on the direct marketing restrictions (in relation to a case (https://www.pcpd.org.hk/english/news_events/media_statements/press_20180102b.html)) determined under the Magistrates’ Court) as follows:

“The Ordinance does not prohibit direct marketing activities. However, organisations must comply with the requirements of the Ordinance when carrying out direct marketing activities. Organisations must obtain a data subject’s consent before using his personal data in direct marketing. Appropriate training must be provided to its staff members to ensure their awareness of and compliance with the direct marketing provisions under the Ordinance.”

In 2018, the Commissioner received 181 direct marketing-related complaints, comparable to 186 cases in 2017. The Commissioner noted that these complaints were mainly regarding:

- the use of personal data for direct marketing without obtaining the data subject’s consent;

- data users failing to observe the data subject’s opt-out request.

In 2018, the Commissioner referred two direct marketing-related cases to the Police that resulted in criminal convictions:

- A supermarket used a data subject’s personal data in direct marketing without obtaining their consent. The supermarket was fined HKD3,000.

- A telecommunications company failed to comply (in two instances) with a data subject’s request to cease using her personal data in direct marketing. The company was fined HKD10,000 for each of the two charges.

In April 2019, an insurance agent was convicted of breaching sections 35C and 35F of the PDPO, for using the personal data of an individual for direct marketing without her consent.

9.5 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?


If the data user plans to use the data received from a third party for direct marketing, the data user is required to follow the PDPO’s direct marketing-related obligations, unless the third party confirms to the data user in writing that:
the third party has given written notice to the data subject and obtained the data subject’s written consent to the provision of personal data; and

- the use of the personal data is consistent with the consent obtained from the data subject.

Oral consent is not possible, and data users must disclose whether or not personal data has been transferred for gain. The above information must be communicated to the data subject in a manner that is easily understandable and if in written form, easily readable. See question 9.1 for further details.

**9.6 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?**

<table>
<thead>
<tr>
<th>Offence</th>
<th>PDPO section</th>
<th>Maximum fine (HK$)</th>
<th>Maximum imprisonment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Using personal data in direct marketing without:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(1) informing the data subject:</td>
<td>35C(5)</td>
<td>500,000</td>
<td>3 years</td>
</tr>
<tr>
<td>- (a) the data user intends to so use the personal data;</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- (b) the data user may not so use the data unless with the data subject’s consent;</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- (c) the kinds of personal data to be used;</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- (d) the classes of marketing subjects which the data is to be used;</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(2) providing the data subject with a response channel for the data subject to communicate consent without charge.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Using personal data in direct marketing without:</td>
<td>35E(4)</td>
<td>500,000</td>
<td>3 years</td>
</tr>
<tr>
<td>(1) having received the data subject’s consent to the intended use;</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(2) having sent a written confirmation to the data subject within 14 days from receiving the consent if given orally, confirming:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- (a) the date of receipt of the consent;</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- (b) the permitted kind of personal data;</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- (c) the permitted class of marketing subjects;</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(3) ensuring the use of the personal data is consistent with the data subject’s consent.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Failing to inform a data subject at the first time of using the personal data in direct marketing that the data user must, without charge, cease to use the data in direct marketing if the data subject so requires.</td>
<td>35F(3)</td>
<td>500,000</td>
<td>3 years</td>
</tr>
<tr>
<td>Failing to comply with the request to cease to use personal data in direct marketing made by a data subject without charge.</td>
<td>35G(4)</td>
<td>500,000</td>
<td>3 years</td>
</tr>
<tr>
<td>Failing to take any of the following actions before providing personal data to another person for direct marketing:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(1) inform the data subject in writing:</td>
<td>35J(5)</td>
<td>1,000,000 (for gain)</td>
<td>5 years (for gain)</td>
</tr>
<tr>
<td>- (a) the data user intends to so provide the personal data;</td>
<td></td>
<td>500,000 (not for gain)</td>
<td>3 years (not for gain)</td>
</tr>
<tr>
<td>- (b) the data user may not so provide the data unless with the data subject’s written consent;</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(2) provide the data subject with written information in relation to:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- (a) where the data is to be provided for gain, that the data is to be so provided;</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- (b) the kinds of personal data to be provided;</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- (c) the classes of persons to which the data is to be provided;</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- (d) the classes of marketing subjects which the data is to be used;</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(3) provide the data subject with a response channel through which the data subject may, without charge, communicate his consent to the intended use.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Providing personal data to another person for direct marketing without:</td>
<td>35K(4)</td>
<td>1,000,000 (for gain)</td>
<td>5 years (for gain)</td>
</tr>
<tr>
<td>(1) having received the data subject’s written consent to the intended provision of personal data;</td>
<td></td>
<td>500,000 (not for gain)</td>
<td>3 years (not for gain)</td>
</tr>
<tr>
<td>(2) if the data is provided for gain, having specified in the information provided to the data subject the intention to so provide; and</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(3) the provision of the data is consistent with the data subject’s consent.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Failing to comply with a data subject’s request to:</td>
<td>35L(6)</td>
<td>1,000,000 (for gain)</td>
<td>5 years (for gain)</td>
</tr>
<tr>
<td>(1) cease to provide the data subject’s personal data for use in direct marketing; or</td>
<td></td>
<td>500,000 (in any other case)</td>
<td>3 years (in any other case)</td>
</tr>
<tr>
<td>(2) notify any data transferee in writing to cease to use the data in direct marketing.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Providing personal data to another person for direct marketing without:</td>
<td>35L(7)</td>
<td>500,000</td>
<td>3 years</td>
</tr>
<tr>
<td>A data transferee failing to comply with a data user’s written notification to cease to use a data subject’s personal data in direct marketing.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
10 **Cookies**

10.1 **Please describe any legislative restrictions on the use of cookies (or similar technologies).**

There is no Hong Kong law that specifically addresses the use of cookies. However, to the extent that cookies are used to store and collect personal data, the PDPO’s relevant provisions would apply. The Commissioner has published Guidance (https://www.pcpd.org.hk/english/publications/files/guidance_internet_e.pdf) that recommends websites that use cookies should explicitly state:

- the type of information that is stored in the cookies;
- whether that information may be transferred; and
- if so, to whom and for what purposes.

In addition, the Commissioner has published Guidance (https://www.pcpd.org.hk/english/publications/files/online_tracking_e.pdf) on the use of online behavioural tracking tools in the context of PDPO compliance.

10.2 **Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?**

This is not applicable in our jurisdiction.

10.3 **To date, has/have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?**

This is not applicable in our jurisdiction.

10.4 **What are the maximum penalties for breaches of applicable cookie restrictions?**

This is not applicable in our jurisdiction.

11 **Restrictions on International Data Transfers**

11.1 **Please describe any restrictions on the transfer of personal data to other jurisdictions.**

There are currently no restrictions in force regarding the transfer of personal data to other jurisdictions.

Section 33 of the PDPO sets out restrictions on the transfer of personal data to other jurisdictions, but it has not yet been enacted and is not operative. If and when it comes into effect, this section would prohibit data transfers to other jurisdictions unless certain conditions are met, including the requirements for the data user to obtain the data subject’s written consent to the transfer and having reasonable grounds to believe that the personal data will be transferred to a jurisdiction that provides a degree of protection as the PDPO.

Section 33 was last discussed (https://www.legco.gov.hk/yr16-17/english/panels/ca/papers/ca20170515cb2-1368-3-e.pdf) in the Legislative Council Panel on Constitutional Affairs in May 2017. The Commissioner has also previously published Guidance (https://www.pcpd.org.hk/english/resources_centre/publications/guidance/files/GN_crossborder_e.pdf) on cross-border data transfer under the PDPO (including model clauses) in December 2014. Some companies have taken the view of mitigating potential disruption by complying with this Guidance and section 33 in its operation (even though it is not yet operative).

11.2 **Please describe the mechanisms businesses typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).**

This is not applicable in our jurisdiction.

11.3 **Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.**

This is not applicable in our jurisdiction.

12 **Whistle-blower Hotlines**

12.1 **What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?**

There is no specific legislation on whistleblowing and there are no restrictions on the types of issues that may be reported. However, the following are relevant to this question:

- various measures exist in relation to the confidentiality of corruption reports to the police and the Hong Kong Independent Commission Against Corruption, with the objective of protecting anonymity and the personal safety of informers, ensuring immunity for witnesses and preventing unfair treatment; and
- section 30A of the Prevention of Bribery Ordinance prevents the names and addresses of informers from being used in civil or criminal proceedings.

12.2 **Is anonymous reporting prohibited, or strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do businesses typically address this issue?**

There is no formal voluntary disclosure programme for claiming amnesty and reduced penalties, though a court and/or authorities may consider any such disclosures (on a case-by-case basis) in determining prosecution and/or penalties. See question 12.1.

13 **CCTV**

13.1 **Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?**

The Commissioner has published Guidance (https://www.pcpd.org.hk/english/publications/files/guidance_cctv_e.pdf) that recommends websites that use cookies should explicitly state:

- the type of information that is stored in the cookies;
- whether that information may be transferred; and
- if so, to whom and for what purposes.

In addition, the Commissioner has published Guidance (https://www.pcpd.org.hk/english/publications/files/online_tracking_e.pdf) on the use of online behavioural tracking tools in the context of PDPO compliance.
13.2 Are there limits on the purposes for which CCTV data may be used?

Pursuant to DPP3, personal data collected from CCTV surveillance should be deleted as soon as practicable after the purpose of collection is fulfilled.

14 Employee Monitoring

14.1 What types of employee monitoring are permitted (if any), and in what circumstances?

There are no specific rules on employee monitoring. To the extent that employee monitoring involves the collection, use and handling of personal data, it would be subject to the PDPO. The Commissioner has published Guidance (https://www.pcpd.org.hk/english/publications/files/monguide_e.pdf) on employee monitoring and personal data privacy in the workplace. The guidelines encourage: employers to evaluate the need for employee monitoring; and offer practical advice on managing personal data obtained from employee monitoring. In general, unless special circumstances exist, employee monitoring should be done in an overt manner. See question 14.2.

14.2 Is consent or notice required? Describe how employers typically obtain consent or provide notice.

The Commissioner encourages employers to prepare an employee monitoring policy that states the purpose for employee monitoring, the circumstances under which employees may be monitored and the purpose for which personal data obtained from monitoring may be used. The employee monitoring policy should be communicated to employees and employers are responsible for safeguarding the protection of employees’ personal data in monitoring records. Consent to monitoring is not required. Consent to use of personal data obtained from monitoring is also not required unless the personal data is used for a purpose other than that stated in the Employee Monitoring Policy or a directly related purpose.

14.3 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?

This is not applicable in our jurisdiction.

15 Data Security and Data Breach

15.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?

Under DPP4, data users must take all practicable steps to protect personal data having particular regard to: the kind of data and the harm that could result if any of those things should occur; the physical location where the data are stored; any security measures incorporated into any equipment in which the data are stored; any measures taken for ensuring the integrity, prudence and competence of persons having access to the data; and any measures taken for ensuring the secure transmission of the data.

15.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expects voluntary breach reporting.

There is no mandatory data breach notification scheme under the PDPO. However:

- The Commissioner has published Guidance (https://www.pcpd.org.hk/english/resources_centre/publications/files/Data_BreachHandling2015_e.pdf) on how to handle data breaches and breach notifications. In this Guidance, and in the event of a personal data breach:
  - the Commissioner recommends voluntary notification by the data user to the Commissioner. Specifically, the Commissioner notes that “[w]hile it is not a statutory requirement on data users to inform the Office of the Privacy Commissioner for Personal Data, Hong Kong about a data breach incident concerning the personal data held by them, data users are nevertheless advised to do so as a recommended practice for proper handling of such incident”; and
  - in relation to any notification to data subjects (where they can be identified), the Commissioner notes that “a data user should consider notifying the data subjects and the relevant parties when real risk of harm is reasonably foreseeable in a data reach. Before making the decision, the consequences for failing to give notification should be duly considered”.
- The Commissioner has also published a template (https://www.pcpd.org.hk/english/publications/files/Notification_Form_e.pdf) data breach notification form, which a data user may use to report a data breach to the Office of the Privacy Commissioner for Personal Data.
- Regulators in certain industries (e.g., financial institutions) may require entities that they regulate to notify data subjects of any data breaches.
15.3 Is there a legal requirement to report data breaches to affected data subjects? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

See question 15.2.

15.4 What are the maximum penalties for data security breaches?

<table>
<thead>
<tr>
<th>Offence</th>
<th>Maximum fine (HK$)</th>
<th>Maximum imprisonment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contravention of an enforcement notice</td>
<td>50,000</td>
<td>2 years</td>
</tr>
<tr>
<td>Contravention of provisions of PDPO (other than as set out in this table)</td>
<td>10,000</td>
<td>6 months</td>
</tr>
<tr>
<td>Direct marketing-related offences</td>
<td>See question 9.6</td>
<td></td>
</tr>
</tbody>
</table>

16 Enforcement and Sanctions

16.1 Describe the enforcement powers of the data protection authority(ies).

See also question 15.4.

The Commissioner can investigate complaints regarding PDPO breaches and initiate investigations. There is scope for criminal enforcement and penalties for non-compliance in certain circumstances.

The Commissioner will first contact the complainant (and potentially the alleged offending data user) to determine if a formal investigation should be undertaken. If the Commissioner commences an investigation and finds that the alleged offender has breached the PDPO, the Commissioner may serve an enforcement notice that directs the offender to take certain steps to remedy the contravention.

Breaching an enforcement notice is an offence under section 50A. The Commissioner can institute civil or criminal proceedings against any data user that breaches an enforcement notice, and can also publish results of any investigation (including naming the data user involved and details of the breach).

In addition to the above, section 66 also provides that a complainant may seek compensation directly from the relevant data user.

16.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?

This is not applicable in our jurisdiction.

16.3 Describe the data protection authority’s approach to exercising those powers, with examples of recent cases.

This is not applicable in our jurisdiction.

16.4 Does the data protection authority ever exercise its powers against businesses established in other jurisdictions? If so, how is this enforced?

See question 3.1.

17 E-discovery / Disclosure to Foreign Law Enforcement Agencies

17.1 How do businesses typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?

Companies generally comply with such requests, subject to any prohibitions under Hong Kong law (e.g. secrecy obligations in the Securities and Futures Ordinance (Cap. 571), prohibiting any persons assisting the Securities and Futures Commission in carrying out their investigations from disclosing anything about the investigation to anyone).

17.2 What guidance has/have the data protection authority(ies) issued?

The Commissioner has not issued any specific guidance on e-discovery or disclosure to foreign law enforcement agencies.
17.2 What Guidance has/have the data protection authority(ies) issued?

The Commissioner has not issued any specific Guidance on e-discovery or disclosure to foreign law enforcement agencies.

18 Trends and Developments

18.1 What enforcement trends have emerged during the previous 12 months? Describe any relevant case law.


- received 16,875 enquiries – an increase of 8% year-on-year. The enquiries mainly related to the collection/use of personal data (e.g. Hong Kong Identity Card numbers or copies) (32%), employment (10%), and use of personal data in direct marketing (6%);
- received 1,890 complaints – an increase of 23% year-on-year. Of these complaints:
  - in terms of the subject of the complaints – 71% were made against the private sector, 12% against the public sector/government departments and 17% against individuals; and
  - in terms of the nature of the complaints – 27% related to the use of personal data without the consent of data subjects, 24% related to the purpose and manner of data collection, 16% related to data security and 5% related to data access/correction requests;
- carried out 289 compliance checks and four investigations – an increase of 14% and 300% year-on-year respectively; and
- received 129 data breach incident reports – an increase of 22% year-on-year.

See also question 18.2.

18.2 What “hot topics” are currently a focus for the data protection regulator?

We have identified several areas of focus throughout this chapter. In the past year, various data privacy-related topics have emerged as key areas of focus for the Commissioner and Hong Kong more generally – owing both to current events and industry/international developments.

The Commissioner’s approach to privacy

In general, the Commissioner’s public comments have indicated that it is increasingly proactive in relation to the PDPO and its enforcement – this has been ongoing since the Commissioner’s release (in February 2014) of the Privacy Management Programme – A Best Practice Guide (https://www.pcpd.org.hk/pmp/files/PMP_guide_e.pdf), which encouraged organisations to (in addition to legal requirements) proactively embrace data protection as part of their corporate governance responsibilities. The Commissioner has particularly focused on the following areas:

- **GDPR**
  - The Commissioner has commented that it is currently reviewing how international privacy legislations (including the APEC Cross Border Privacy Rules) align with the PDPO. In April 2018, the Commissioner issued the European Union General Data Protection Regulation (“GDPR”) 2016 booklet, in order to prepare businesses for the GDPR that came into force on 25 May 2018.
  - The GDPR explicitly requires compliance by organisations established in non-EU jurisdiction in certain situations. Compliance with the GDPR is an increasing area of concern for Hong Kong-based organisations, and we have noticed an uptick in GDPR-related enquiries, both before and after 25 May 2018. The Commissioner recently announced that it received three GDPR-related complaints in 2018.

- **Drones**
  - As the use of drones is increasingly prevalent, the Commissioner reiterated the importance of compliance with the PDPO should collection of personal data be involved. In 2018, the Commissioner held discussions with related government departments in the context of the public consultation on regulation of unmanned aircraft systems, and made recommendations in relation to privacy protection.

- **Reforming the PDPO**
  - The Commissioner has continued to make public comments regarding reforms of the PDPO. In particular, the Commissioner in February 2019 commented on the following (https://www.hongkongfp.com/2019/02/01/data-breacher-hit-record-high-2018-says-hong-kongs-privacy-watchdog/):
    - The Commissioner will discuss PDPO reforms with the Hong Kong government in the first half of 2019, with talks nearing final stages.
    - The Commissioner acknowledged that the public’s concern regarding mandatory reporting requirements, the PCPD’s enforcement powers, penalties for data breaches, and regulations on data users.
    - While the Commissioner can issue warnings and enforcement notices under the PDPO, it has no powers of criminal investigation or prosecution. Such powers may be part of any reform from the Legislative Council.
    - The Commissioner noted that the number of PCPD staff had remained the same over the past decade, and called on the Hong Kong government to increase the 69-person team by at least half, in order to cope with future workload.
    - In addition, the Commissioner has separately stated that it is engaging with privacy regulators across the globe to seek solutions on how information is shared, with a particular focus on multinational organisations, and to ensure that no regulator is “reinventing the wheel”.

- **Data ethics**
  - The Commissioner is undertaking increasing work in relation to data ethics. Most notably:
    - The PCPD issued the Ethical Accountability Framework for Hong Kong, China in October 2018. The Framework focused, in particular, on three Data Stewardship Values of data ethics – “Respectful, Beneficial and Fair”.
    - The PCPD was amongst various international data protection authorities who issued the Declaration on Ethics and Data Protection in Artificial Intelligence, at the International Conference of Data Protection and Privacy Commissioners in October 2018.
    - In May 2018, the Commissioner issued an information leaflet for small and medium-sized enterprises (“SMEs”), including a series of questions for Ethical Data Impact Assessment.

The Commissioner has stated that, in addition to complying with the PDPO:

- Organisations should carry out Ethical Data Impact Assessment before engaging in activities related to big data analysis and artificial intelligence.
- Data ethics is focused on “offering individuals genuine choices, meaningful consent, equality and non-discrimination. Most importantly, it gives back the right to self-determination in the use of personal data to the data subjects.”
The HKMA has separately issued a letter to banks on 3 May 2019, encouraging banks to adopt the PCPD’s Ethical Accountability Framework.

- **Strategic objectives for the Commissioner in 2019**
  
  More generally, the Commissioner has stated that it will be focusing on the following strategic objectives in 2019:
  
  - continue to enforce the law fairly, promote, and educate all stakeholders about personal data protection;
  - continue to engage organisations (especially SMEs) in promoting compliance in protecting personal data and implementing the privacy governance mechanisms and data ethics;
  - strengthen the working relationship with the mainland and overseas data protection authorities to handle cross-jurisdiction data contravention incidents, and explain the newly implemented rules and regulations on data protection of other jurisdictions to the local stakeholders for compliance with the requirements; the free flow of information and privacy protection being one of Hong Kong’s unique and irreplaceable attributes;
  - facilitate, in accordance with the law organisations, including the government, initiatives involving personal data privacy, including making recommendations on the review of the Ordinance; and
  - issue guidance on “Fintech” and “de-identification” and publish a booklet on major personal data regulations in the mainland for industries and members of the public.

Meanwhile, awareness of data privacy has been increasing amongst both regulators and the Hong Kong public, for various reasons.

- **Financial services regulators, data privacy, cybersecurity and open banking**
  
  Both the Commissioner and industry regulators (particularly financial services regulators) have been increasingly focused on cybersecurity-related issues and initiatives. For example:
  
  - in December 2016, the HKMA announced a new Cyber Fortification Initiative to improve the cyber resilience of its Authorised Institutions;
  - in October 2017, the SFC issued guidelines and baseline requirements for licensed or registered persons engaged in internet trading, to enhance cybersecurity and mitigate hacking risks;
  - in April 2018, the HKMA fully launched the Cyber Intelligence Sharing Platform – which facilitates the sharing of cyber threat intelligence by banks;
  - in November 2018, the HKMA announced the revised Guide to Enhanced Competency Framework on Cybersecurity, which sets out the competency standards for cybersecurity practitioners in the Hong Kong banking industry;
  - in November 2018, the SFC publicly commented that it will soon conduct surveys and inspections of licensed entities to assess their compliance with various cybersecurity requirements; and
  - in January 2019, the HKMA stated that its objectives in relation to operational resilience and technology risk management include cyber resilience and recovery; supervision of virtual banks; “regtech”; and implementing Open API.

In our view, financial services regulators, in particular, will increasingly become secondary regulators of data privacy, after the Commissioner. In particular, with:

- the HKMA having announced eight new licensees under the virtual banking regime, and
- Hong Kong’s version of Open Banking likely to make significant progress in 2019 and beyond (including in relation to the sharing of personal data between data subjects, traditional banks and new fintechs/other third-party service providers), regulators, industry players and data subjects are all becoming increasingly aware of the value and portability of personal data, and risks arising from that. We will be keeping a close eye on this issue in 2019 and beyond.

- **Data breaches**
  
  There were a number of high-profile data breaches in Hong Kong during 2018, that led to significant public attention on data privacy. The Commissioner announced in February 2019 that Hong Kong saw a record number of user data breaches in 2018, with 129 such incidents reported to the Commissioner. Significant reported data breaches in Hong Kong include:
  
  - in November 2017 and January 2018 – hacks into various travel agencies’ databases of personal information, affecting over 200,000 customers;
  - in April 2018 – a hack into an inactive database owned by Hong Kong Broadband Network which held personal information on 380,000 customers; and
  - in November 2018 – TransUnion’s Hong Kong entity suspended its online services after a local newspaper was able to access various high-profile public figures (while not being regulated by any official body in Hong Kong) and subsequent pressure from various Hong Kong government bodies.

The most high-profile data breach in 2018, by far, affected passengers of Cathay Pacific and its subsidiary Hong Kong Dragon Airlines. In total, various personal data of 9.4 million passengers were leaked – with the personal data relating to a combination of passengers’ names, nationalities, dates of birth, telephone numbers, emails, physical addresses, passport numbers, identity card numbers, frequent flyer programme membership numbers, customer service remarks and travel history. Cathay initially detected suspicious activity in March 2018 and confirmed the breach in May 2018 – but did not disclose the breach until 25 October 2018. The Commissioner has subsequently launched an investigation into the Cathay data breach, but while it is intent on carrying out a “detailed compliance investigation” into that breach, the Cathay data breach in particular has prompted significant media and public commentary and review of a number of aspects regarding the PDPO – including:

- The lack of significant penalties for breaches of the PDPO, particularly as compared to the GDPR and other overseas data privacy laws.
- The lack of a mandatory statutory requirement that data breaches be reported. While data controllers are required to protect data subjects’ privacy rights in various ways under the PDPO, the PDPO operates a voluntary data breach reporting regime.
- Whether the PDPO and its requirements are falling significantly behind the rest of the world – given that it was first enacted in 1996 and last updated in 2012. While the Commissioner has previously made public statements regarding updating the PDPO (see above), to date no substantive consultations or other public moves regarding a new data privacy law have been announced.
CCTV cameras and personal privacy

In April 2019, the Hong Kong newspaper Apple Daily published intimate footage showing Hong Kong singer Andy Hui and actress Jacqueline Wong in the back seat of a moving car. The footage appears to have been taken from that taxi’s CCTV camera, which was pointed at the back seat. To date, the video’s creator/supplier has not been identified. While the car appears to have been a taxi, that has also not been confirmed.

The Commissioner has publicly stated the following:

“If a camera is installed inside a taxi to collect the image or audio of passengers, and if the recorded image can be used to identify individuals, then the taxi driver or company must follow the Personal Data (Privacy) Ordinance and its six data protection principles. If such videos were used for a purpose not originally intended, such as dissemination on the internet, then it would be a breach of the passengers’ privacy.”

In this case, it appears that the six principles have not been followed – particularly in relation to notification to data subjects regarding the occurrence of data collection and the usage of personal data in a lawful and fair manner.

While there was significant public attention focused on the two data subjects, many also focused on the data privacy aspects of this matter. In particular:

■ While Macau has a law regarding only video and audio devices that were installed by the Macau Transport Bureau being permitted for use in taxis, Hong Kong has no such laws (the Hong Kong Transport Bureau will issue voluntary guidelines later in 2019). There was significant public concern about the potential use of such CCTV footage in taxis and other public transportation methods, and increasing regulatory attention on this aspect is likely – including regulating what videos are used and who can access such footage (e.g. whether such footage should be encrypted and only accessed by the relevant authorities).

■ Under the PDPO, affected parties can complain to the Commissioner – but issuing an enforcement notice to the taxi driver in question/Apple Daily (after the fact), even if they have breached the PDPO, is unlikely to be of much help to the data subjects in question, particularly given the relatively insignificant penalties available. The Commissioner has publicly stated that while it appears this matter was an infringement of the two data subjects’ rights under the PDPO, it can only pursue any investigation if the data subjects in question filed a complaint; and the Commissioner subsequently stated that the data subjects have indicated they will not be filing a complaint.

■ Meanwhile, Hong Kong government departments and corporations were quick to issue various advertisements that appear to be satirising and/or mocking the incident. This has led to concerns over whether such responses were appropriate and what they meant for the government’s wider attitude towards data privacy.
Joshua Cole
Ashurst Hong Kong
11/F Jardine House
1 Connaught Place
Hong Kong
Tel: +852 2846 8989
Email: joshua.cole@ashurst.com
URL: www.ashurst.com

Joshua is Managing Partner of the Ashurst Hong Kong office and leads our Digital Economy practice in Asia.

Joshua has over 20 years of experience advising on TMT and related corporate and commercial matters, to clients in TMT and other sectors – including financial services, energy and resource, pharmaceutical and retail. He has advised on a number of high-profile international acquisitions, disposals and joint ventures involving Hong Kong, China, Japan, Myanmar, Korea, the Philippines and other South East Asian countries. He also advises telecommunications businesses on commercial and regulatory matters in Asia, including network build agreements and spectrum acquisitions/licensing.

Joshua has been named by Chambers Asia Pacific as a leading TMT lawyer, and is the author of various M&A and telecommunications law-related publications.

Hoi Tak Leung
Ashurst Hong Kong
11/F Jardine House
1 Connaught Place
Hong Kong
Tel: +852 2846 8982
Email: hoitak.leung@ashurst.com
URL: www.ashurst.com

Hoi is Counsel in the Ashurst Hong Kong office.

Hoi brings a wealth of experience on technology and IP-related matters across Asia. He has advised a broad spectrum of clients from multinational corporations to start-ups, spanning from TMT to other sectors such as financial services, insurance, entertainment, education and retail. His practice includes advising on:

- transaction structuring, contract drafting and negotiations – including: outsourcing, procurement, supply and distribution arrangements; technology and content licensing, use and development; launch/ expansion of B2B and B2C technology services; cloud computing, data centre and telecommunications/network infrastructure projects; and BAU commercial agreements;
- TMT/IP/data-focused corporate transactions – including: M&As; JVs; and restructurings; and
- TMT-related issues – including: fintech; cryptocurrencies; cybersecurity; data privacy and big data arrangements; and emerging technologies and businesses (e.g. blockchain, smart contracts, artificial intelligence and e-sports) in various industry sectors.

Hoi works closely with the Ashurst Advance team – with a particular interest in legal service innovation through technology (including automation of legal tasks and smart contracts). He writes frequently, and is regularly quoted by the media on technology law-related topics.

Ashurst is a leading global law firm with a rich history spanning almost 200 years. We currently have 26 offices in 16 countries and a number of referral relationships that enable us to offer the reach and insight of a global network, combined with the knowledge and understanding of local markets. With over 400 partners and a further 1,450 lawyers working across 10 different time zones, we are able to respond to our clients wherever and whenever they need us.

We believe our legal expertise is impeccable, reflected in our experience with technology-focused transactions worldwide, working with some of the world’s most successful digital economy companies. We particularly focus on:

- Being approachable, practical and commercially minded.
- Taking a multi-disciplinary approach and working as a team.
- Understanding our clients and their industry-specific issues.
- Clarity and transparency in communication.
- Always innovating to provide the most effective and efficient service.
- Diversity of personnel.
- Transparency and efficiency in our costs.
- Always focusing on people – a human-first approach.

We work with clients across the spectrum – from large to small, in different industries and all parts of the world, all revolving around the complex legal issues arising from the intersection of technology and law.

Most importantly, we focus on helping you grow and be successful – no matter what stage of business you are at.
Chapter 19

India

Subramaniam & Associates (SNA)

1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

In the absence of specific legislation, data protection is achieved in India on the basis of the following legislation, which also applies to other aspects of online regulation, such as e-commerce and cybercrime.

The Information Technology Act (2000), amended by the Information Technology (Amendment) Act (2008) (henceforth “the IT Act”) which contains provisions for the protection of electronic data. The IT Act penalises “cyber contraventions” which attract civil prosecution under section 43 (a) to (h) and “cyber offences” which attract criminal action under sections 63 to 74. The former category includes gaining unauthorised access to, and downloading or extracting data from, computer systems or networks. The latter covers “serious” offences like tampering with computer source code, hacking with intent to cause damage and breach of confidentiality and privacy.

In April 2011, the Indian Ministry of Communications and Technology published four sets of rules implementing certain provisions of the Information Technology (Amendment) Act (2008). Of relevance to the issue of data protection are The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules (2011) (henceforth “the SPD Rules”). The SPD Rules were framed under section 43A of the IT Act, and set out procedures for corporate entities which collect, process or store personal data (including sensitive personal information). These Rules also distinguish “personal information” from “sensitive personal information”.

The IT Act was not drafted specifically with the protection of data in mind. Therefore, the patchwork of existing legislation being used for this purpose leaves a lot to be desired in terms of effective protection of data and even basic definitions of scope and sanctions. The SPD Rules are specific to data protection, but technological growth has significantly outstripped this piece of legislation, rendering certain definitions in the Rules too narrow to be effective and leaving some categories of personal data entirely outside statutory scope.

Draft legislation called the Privacy Bill was released in 2011, which recognised an individual’s right to privacy. Various iterations of this bill were released over six years, the most recent of which was the Data Privacy Bill, 2017. However, this bill did not pass into law. Subsequently, the Supreme Court recognised the right to privacy as a constitutionally guaranteed fundamental right in 2017. In August 2017, the government empanelled a ten-member committee of experts under the chairmanship of a retired Supreme Court judge. The mandate for the committee was “to identify key data protection issues in India and recommend methods of addressing them”. The committee submitted a nearly 200-page report containing a “data protection framework” along with the draft Personal Data Protection Bill, 2018, little over a year later. After several rounds of consultation with various stakeholders, including the US government, the revised draft will likely be tabled before Parliament later this year.

As will become evident from many of the answers below, should the Personal Data Protection Bill, 2018 come into force, it will make some significant changes to the existing legal position on privacy and data protection in India. It appears that the draft Personal Data Protection Bill, 2018 is intended as a replacement for the Data Privacy Bill, 2017, despite the fact that both draft pieces of legislation cover separate aspects of privacy and data protection. Neither is currently the law of the land. Although there is some overlap between various iterations of the Data Privacy Bill and the draft Personal Data Protection Bill, 2018, the answers below make reference to the Data Privacy Bill, 2017 only if neither the current laws nor the draft Personal Data Protection Bill, 2018, address the issues raised in the question and the Draft Privacy Bill, 2017 does.

1.2 Is there any other general legislation that impacts data protection?

Data protection may sometimes occur through the following:

- The Copyright Act (1957): Since the Act protects intellectual property rights in different types of creative work including literary works, and the term “literary work” statutorily includes computer databases, copying a computer database, or copying or distributing, a database could amount to copyright infringement under the Act. This provides some scope for protecting different types of data as “literary works”. Obviously, there is a difference between database protection and data protection. Database protection protects the creative investment in compilation, presentation and verification of databases, while data protection aims to protect the privacy of individuals by limiting or restricting access to their personal or sensitive information.

- The Indian Penal Code (1860): This could be used to prevent theft of data. The offences of theft and misappropriation technically apply only to movable property under the Indian Penal Code, but the term “movable property” has been defined to include corporeal property of every description except land or property that is permanently attached to the earth.

- The Indian Constitution: Article 21 of the Constitution protects an individual’s right to life and personal liberty. The Supreme Court of India, in a nine-judge bench decision in
August 2017, held that citizens enjoy a fundamental right to privacy that is intrinsic to life and liberty. Article 300A of the Constitution also guarantees the right not to be deprived of one's property except by authority of law, so if the data in question is regarded as property, this provision may be relied upon. It must be noted, however, that rights guaranteed by the Constitution may normally only be used against the State or State-owned enterprises.

In addition to the above, invasion or breach of privacy could lead to an action in tort.

### 1.3 Is there any sector-specific legislation that impacts data protection?

The National Association of Service & Software Companies (NASSCOM) – a not-for-profit industry association and the apex body for the Indian IT BPM industry – spearheads private sector initiatives to protect and bolster data privacy regulation in India.

Business Process Outsourcing Units implement self-regulatory processes, such as the BS 7799 and the ISO 17799 standards, to standardise information security management and restrict the quantity of data made available to employees.

The Reserve Bank of India periodically issues guidelines, regulations and circulars to maintain the confidentiality and privacy of client information, and in 2006, in conjunction with several other banks belonging to the Indian Banks Association, also established a body called the Banking Codes and Standards Board of India to evolve a set of voluntary norms which banks must enforce themselves through internal grievance redressal mechanisms within each bank. These mechanisms include a designated “Code Compliance Officer” and an Ombudsman.

The Medical Council of India has set out the Indian Medical Council (Professional conduct, Etiquette and Ethics) Regulations, 2002 (Code of Ethics Regulations, 2002). These rules govern various issues, including doctor-patient confidentiality, the collection of personal data from patients, issues of consent, and the extent to which invasive procedures may be conducted.

Similarly, the Securities and Exchange Board of India is a securities market regulator which requires securities market intermediaries to maintain confidentiality of client data, including personal data.

These regulations apply in addition to the IT Rules. While they provide a certain degree of security, the lack of legislative enforcement and foresight mean that they are enforced in varying degrees by each individual institution and do not come with guaranteed parliamentary sanction.

### 1.4 What authority(ies) are responsible for data protection?

No state or central authorities have yet been designated purely for the enforcement and regulation of data protection laws, although any plaintiffs have the right and opportunity to bring a matter of concern to a court with suitable jurisdiction.

In cases where the compensation amount claimed for a failure to protect confidentiality of sensitive personal information is less than INR 50,000,000, the IT Act provides for the Government to appoint an Adjudicating Officer. All proceedings before the Adjudicating Officer are deemed to be judicial proceedings and the officer has the powers of a civil court. The details of the enquiry procedure that the Adjudicating Officer must use are provided in the Information Technology (Qualification and Experience of Adjudicating Officers and Manner of Holding Enquiry) Rules (2003).

The Personal Data Protection Bill, 2018 (“the PDPB”) contemplates the establishment and incorporation of a Data Protection Authority by the Central Government. As envisaged in Section 50 of the PDPB, said Authority will comprise of six full-time members appointed for a five-year term by the Central Government. Appointments will be made on recommendation by a selection committee consisting of the Cabinet Secretary, the Chief Justice of India or a Supreme Court Justice nominated by the Chief Justice, and “one expert of repute” nominated by the Cabinet Secretary and Chief Justice. Section 60 of the PDPB details the powers and functions of the Authority, which include a wide range of functions related to monitoring data transfers and fiduciaries involved in such transfers, enforcement of the law and of its own codes of practice, which it will be empowered to write, taking action in response to data breaches, creating a rating for fiduciaries in the form of a “data trust score”, advising Parliament and Central and State governments, etc.

### 2 Definitions

#### 2.1 Please provide the key definitions used in the relevant legislation:

- **“Personal Data”**
  
  The legislation does not contain a definition for the term “personal data”. However, the IT Rules define “personal information” as any information that relates to a natural person, which, either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such a person.

  The IT Act defines “data” as a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalised manner, and is intended to be processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts, magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer.

  The PDPB defines “personal data” as follows: “data about or relating to a natural person who is directly or indirectly identifiable, having regard to any characteristic, trait, attribute or any other feature of the identity of such natural person, or any combination of such features, or any combination of such features with any other information”.

- **“Processing”**
  
  Neither the IT Act nor the IT Rules contain a definition of the term “processing”.

  The PDPB defines “processing” as follows: “…in relation to personal data [processing] means an operation or set of operations performed on personal data, and may include operations such as collection, recording, organisation, structuring, storage, adaptation, alteration, retrieval, use, alignment or combination, indexing, disclosure by transmission, dissemination or otherwise making available, restriction, erasure or destruction”.

- **“Controller”**
  
  Neither the IT Act nor the IT Rules contain a definition of the term “data controller”.

  The Privacy Bill, 2011 did define the term as any person who processes personal data. This includes bodies corporate, partnerships, societies, trusts, associations of persons, Government companies, Government departments, urban local bodies, agencies or instruments of the State.

  Additionally, the Data Privacy Bill, 2017 defined the term as a person who, either alone or jointly or in combination with
other persons, determines the purposes for which and the manner in which any personal data are used, or are to be, processed.

The PDPB defines “data fiduciary” as “any person, including the State, a company, any juristic entity or any individual who alone or in conjunction with others determines the purpose and means of processing of personal data”.

■ “Processor”
Neither the IT Act nor the IT Rules contain a definition of “processor” or “data processor”.

The PDPB defines “data processor” as “any person, including the State, a company, any juristic entity or any individual who processes personal data on behalf of a data fiduciary, but does not include an employee of the data fiduciary”.

■ “Data Subject”
In August 2011, the Ministry of Communications and Information issued a “Press Note” (Clarification on the Privacy Rules) which states that the term “provider of information” refers to those natural persons who provide sensitive personal data or information to a body corporate. It is generally understood that “provider of information” is synonymous with “data subject”, although the legislation contains no definition of either term.

According to the Privacy Bill, 2011, a data subject is any living individual whose personal data is processed by a data controller in India.

The PDPB does not refer to a data subject either, but defines “data principal” as the natural person to whom the personal data referred to in the bill relates.

■ “Sensitive Personal Data”
The IT Rules define “sensitive personal data or information” as such personal information which consists of information relating to:

■ passwords;
■ financial information, such as bank account or credit card or debit card or other payment instrument details;
■ physical, physiological and mental health conditions;
■ sexual orientation;
■ medical records and history;
■ biometric information;
■ any details relating to the above clauses as provided to a body corporate for provision of services; and
■ any information received under the above clauses by a body corporate for processing, or which has been stored or processed under lawful contract or otherwise.

Provided that any information that is freely available or accessible in the public domain, or furnished under the Right to Information Act (2005), or any other law currently in force, shall not be regarded as sensitive personal data or information for the purposes of these rules.

The PDPB similarly defines “sensitive personal data” as “[personal data revealing, related to, or constituting, as may be applicable - (i) passwords; (ii) financial data; (iii) health data; (iv) official identifier; (v) sex life; (vi) sexual orientation; (vii) biometric data; (viii) genetic data; (ix) transgender status; (x) intersex status; (xi) caste or tribe; (xii) religious or political belief or affiliation; or (xiii) any other category of data specified by the Authority under section 22)” where the Authority is the data protection authority envisaged by the bill, and section 22 of the bill empowers said authority to specify such further categories of sensitive personal data as it deems necessary based on the need for additional safeguards or restrictions.

■ “Data Breach”
Neither the IT Act nor the IT Rules contain a definition of the term “data breach”.

According to the Data Privacy Bill, 2017, a “data breach” includes any unauthorised access, destruction, use, processing, storage, modification, de-anonymisation, unauthorised disclosure (either accidental or incidental) or other reasonably foreseeable risks or data security breaches of personal data. The PDPB does not define “data breach”, but does define “personal data breach” as any unauthorised or accidental disclosure, acquisition, sharing, use, alteration, destruction, loss of access to, of personal data that compromises the confidentiality, integrity or availability of personal data to a data principal”.

Other key definitions – please specify (e.g., “Pseudonymous Data”, “Direct Personal Data”, “Indirect Personal Data”).

The Act and Rules do not contain definitions for these terms, and neither does the PDPB. However, the PDPB does contain other important definitions, the most crucial of which deal with consent.

The PDPB states that “consent” shall mean consent under section 12 of the PDPB. Section 12 in turn states the following:

■ “Processing of personal data on the basis of consent:

(1) Personal data may be processed on the basis of the consent of the data principal, given no later than at the commencement of the processing.

(2) For the consent of the data principal to be valid, it must be:

(a) free, having regard to whether it meets the standard under section 14 of the Indian Contract Act, 1872 (9 of 1872);

(b) informed, having regard to whether the data principal has been provided with the information required under section 8;

(c) specific, having regard to whether the data principal can determine the scope of consent in respect of the purposes of processing;

(d) clear, having regard to whether it is indicated through an affirmative action that is meaningful in a given context; and

(e) capable of being withdrawn, having regard to whether the ease of such withdrawal is comparable to the ease with which consent may be given.

(3) The data fiduciary shall not make the provision of any goods or services or the quality thereof, the performance of any contract, or the enjoyment of any legal right or claim, conditional on consent to processing of any personal data not necessary for that purpose.

(4) The data fiduciary shall bear the burden of proof to establish that consent has been given by the data principal for processing of personal data in accordance with sub-section (2).

(5) Where the data principal withdraws consent for the processing of any personal data necessary for the performance of a contract to which the data principal is a party, all legal consequences for the effects of such withdrawal shall be borne by the data principal.”

The PDPB also differentiates “consent” from “explicit consent” in section 18 of the PDPB, as follows:

■ “Processing of sensitive personal data based on explicit consent:

(1) Sensitive personal data may be processed on the basis of explicit consent.

(2) For the purposes of sub-section (1), consent shall be considered explicit only if it is valid as per section 12 and is additionally:

(a) informed, having regard to whether the attention of the data principal has been drawn to purposes of or operations in processing that may have significant consequences for the data principal;
(b) clear, having regard to whether it is meaningful without recourse to inference from conduct in a context; and
(c) specific, having regard to whether the data principal is given the choice of separately consenting to the purposes of, operations in, and the use of different categories of sensitive personal data relevant to processing.”

3 Territorial Scope

3.1 Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to those laws?

Yes, section 75 of the IT Act states that the provisions of the Act would apply to any offence or contravention thereunder committed outside India by any person (including companies), irrespective of his nationality, if the act or conduct constituting the offence or contravention involves a computer, computer system or computer network located in India.

As far as the PDPB is concerned, it will apply to entities outside the territories of India to the extent that any cross-border data transfers outward from India may be regulated by the Central Government (should it come into force). The PDPB prescribes in section 41, subsection 2, that the Central Government shall be entitled to permit such transfers only where it finds that the relevant personal data shall be subject to an adequate level of protection, having regard to the applicable laws and international agreements, and the effectiveness of the enforcement by authorities with appropriate jurisdiction. The PDPB also prescribes that the Central Government shall monitor the circumstances applicable to such data in order to review such decisions.

The PDPB also states in section 104 that the Central Government may, by notification, render exempt from its application, the processing of personal data of data principals not within the territory of India, by any data processor or any class of data processors incorporated under Indian law. This implies that outside the territory of India, including any company incorporated outside the territory of India, by any data processor or any class of data processors incorporated under Indian law. This implies that outside the territory of India, any person (including companies), irrespective of his nationality, if the act or conduct constituting the offence or contravention involves a computer, computer system or computer network located in India.

As far as the PDPB is concerned, it will apply to entities outside the territories of India to the extent that any cross-border data transfers outward from India may be regulated by the Central Government (should it come into force). The PDPB prescribes in section 41, subsection 2, that the Central Government shall be entitled to permit such transfers only where it finds that the relevant personal data shall be subject to an adequate level of protection, having regard to the applicable laws and international agreements, and the effectiveness of the enforcement by authorities with appropriate jurisdiction. The PDPB also prescribes that the Central Government shall monitor the circumstances applicable to such data in order to review such decisions.

The PDPB also states in section 104 that the Central Government may, by notification, render exempt from its application, the processing of personal data of data principals not within the territory of India, by any data processor or any class of data processors incorporated under Indian law. This implies that outside the territory of India, including any company incorporated outside the territory of India, by any data processor or any class of data processors incorporated under Indian law. This implies that outside the territory of India, any person (including companies), irrespective of his nationality, if the act or conduct constituting the offence or contravention involves a computer, computer system or computer network located in India.

This is true even if the data principal is also not within the Indian jurisdiction.

4 Key Principles

4.1 What are the key principles that apply to the processing of personal data?

Transparency

Under the IT Rules, data controllers and data processors must provide a privacy policy for the handling of or dealing in personal information, including sensitive personal information, and ensure that this policy is available to the data subject who has provided said information by lawful contract. Further, the policy shall be published on the website of the body corporate or any person on its behalf, and shall provide:

1. clear and easily accessible statements of the practices and policies of the data controller;
security. Any reasonable purposes must be specified by the data protection authority envisaged by the PDPB (please see answer to question 1.4) and the considerations to be taken into account when it elects to do so are also provided for by the PDPB. These include the public interest, the reasonable expectations of the data principal and whether the data fiduciary can reasonably be expected to obtain consent.

- The PDPB also states in section 7 that sensitive personal data may only be lawfully processed on the basis of one or more grounds provided in Chapter IV of the PDPB. Chapter IV defines "explicit consent" which is required for such lawful processing (please see the answer to question 2.1) and then provides for the available grounds for the lawful processing of sensitive personal data:
  i. for functions of the State;
  ii. for compliance with law or any order of a court or tribunal;
  iii. when necessary for prompt action; or
  iv. for the lawful processing of further categories of sensitive personal data as may be specified by the data protection authority envisaged by the PDPB (please see answer to question 1.4) on the basis of further grounds as may be specified by the authority. The considerations to be taken into account by the authority in such circumstances include the risk of significant harm to the data principal, the expectation of confidentiality attached to the category of sensitive personal data and the potential suffering of a significantly discernible class of data principals. The authority is also empowered to "specify categories of personal data, which require additional safeguards or restrictions where repeated, continuous or systematic collection for the purposes of profiling takes place and, where such categories of personal data have been specified, the Authority may also specify such additional safeguards or restrictions applicable to such processing".

- **Purpose limitation**

  The IT Rules or the Act do not provide a specific time frame for the retention of sensitive personal information. However, the IT Rules state that a body corporate or any person on its behalf holding sensitive personal data or information shall not retain that information for longer than is required for the purposes for which the information may lawfully be used or is otherwise required under any other law for the time being in force.

  The PDPB states the following in section 5 with regard to purpose limitation:
  
  "(1) Personal data shall be processed only for purposes that are clear, specific and lawful.

  (2) Personal data shall be processed only for purposes specified or for any other incidental purpose that the data principal would reasonably expect the personal data to be used for, having regard to the specified purposes, and the context and circumstances in which the personal data was collected."

  The PDPB also states in section 6:

  "Collection limitation – Collection of personal data shall be limited to such data that is necessary for the purposes of processing."

- **Data minimisation**

  There is no statutory definition or guidance with respect to data minimisation.

- **Proportionality**

  There is no statutory definition or guidance with respect to proportionality.

- **Retention**

  The IT Rules and the IT Act do not provide specific guidance with respect to the time frame for retention of sensitive personal information. However, the Rules do not override provisions of other laws that may specify a maximum period of retention for sensitive data. For example, telecom licenses require licensees to maintain, for security reasons and for scrutiny by the Department of Telecommunication, all commercial records related to communications exchanged on the network for at least one year.

  Section 67C of the IT Act requires an intermediary to preserve and retain information, in a manner and format and for such period of time, as may be prescribed by the Central Government. "Intermediary" includes telecom service providers, network service providers, internet service providers, web-hosting service providers, search engines, online auction sites, online marketplaces and cyber cafés. The Central Government has yet to frame rules implementing the retention provision under section 67C.

  The PDPB states in section 10 that data fiduciaries may retain personal data only for as long as is "reasonably necessary to satisfy the purpose for which it is processed." However, should retention for a longer duration be mandated or necessary to comply with legal obligations, the PDPB permits such retention. Further, the PDPB requires that the data fiduciary undertake periodic reviews to assess the continued necessity of retaining the personal data in question and delete said data when it is no longer necessary to retain it. In section 61, when outlining the powers of the data protection authority, the PDPB also provides for the authority to issue a code of practice for "measures pertaining to the retention of personal data under section 10".

  **Other key principles – please specify**

  There are no other key principles.

### 5 Individual Rights

#### 5.1 What are the key rights that individuals have in relation to the processing of their personal data?

- **Right of access to data/copies of data**

  Rule 5, subsection 6 of the IT Rules mandates that the body corporate or any person on its behalf must permit providers of information or data subjects to review the information they may have provided. However, the Rules do not explain the procedure to be followed by data subjects in exercising the right to access the data they have provided. It also does not detail whether there is a time limit within which the data processor must comply with a request for access.

  The PDPB states the following in section 24:

  "Right to confirmation and access:

  (1) The data principal shall have the right to obtain from the data fiduciary:

  (a) confirmation whether the data fiduciary is processing or has processed personal data of the data principal;

  (b) a brief summary of the personal data of the data principal being processed or that has been processed by the data fiduciary; and

  (c) a brief summary of processing activities undertaken by the data fiduciary with respect to the personal data of the data principal, including any information provided in the notice under section 8 in relation to such processing activities."
(2) The data fiduciary shall provide the information as required under this section to the data principal in a clear and concise manner that is easily comprehensible to a reasonable person."

According to section 28 of the PDPB, any rights enforced by the data principal under the PDPB, with the exception of the right to be forgotten under section 27, must be exercised via a request made in writing to the data fiduciary. Section 28 requires that the data fiduciary be provided with a reasonable amount of information so as to satisfy itself as to the identity of the data principal making the request, acknowledge receipt within a specified period of time, and be permitted to charge a reasonable fee for certain requests (with some exceptions).

■ Right to rectification of errors

As far as current law is concerned, the answer to this question may be provided together with the answer to the "right to deletion/right to be forgotten"; see below.

In the PDPB, however, the right to rectification of errors is treated separately from the right to be forgotten. Section 25 of the PDPB states the following:

"Right to correction, etc.:

(1) Where necessary, having regard to the purposes for which personal data is being processed, the data principal shall have the right to obtain from the data fiduciary processing personal data of the data principal;
(a) the correction of inaccurate or misleading personal data;
(b) the completion of incomplete personal data; and
(c) the updating of personal data that is out of date.

(2) Where the data fiduciary receives a request under sub-section (1), and the data fiduciary does not agree with the need for such correction, completion or updating having regard to the purposes of processing, the data fiduciary shall provide the data principal with adequate justification in writing for rejecting the application.

(3) Where the data principal is not satisfied with the justification provided by the data fiduciary under sub-section (2), the data principal may require that the data fiduciary take reasonable steps to indicate, alongside the relevant personal data, that the same is disputed by the data principal.

(4) Where the data fiduciary corrects, completes, or updates personal data in accordance with sub-section (1), the data fiduciary shall also take reasonable steps to notify all relevant entities or individuals to whom such personal data may have been disclosed regarding the relevant correction, completion or updating, particularly where such action would have an impact on the rights and interests of the data principal or on decisions made regarding them."

Procedures outlined under section 28 of the PDPB would apply in the enforcement of this right (see answer on the right to access of data, above).

■ Right to deletion/right to be forgotten

Rule 5, subsection 6 of the IT Rules states that data subjects must be allowed access to the data provided by them and ensure that any information found to be inaccurate or deficient shall be corrected or amended as feasible. Although the Rules do not directly address deletion of data, they state in Rule 5, subsection 1, which corporate entities or persons representing them must obtain written consent from data subjects regarding the usage of the sensitive information they provide. Further, data subjects must be provided with the option not to provide the data or information sought to be collected.

In section 27, the PDPB provides the data principal with the right to restrict or prevent continuing disclosure of personal data by the data fiduciary, should they believe that the purpose for which it was disclosed has been served, or that consent on the basis of which the personal data was shared has been withdrawn, or if the disclosure was made contrary to the provisions of the PDPB. While section 27 is entitled “Right to be Forgotten”, there is no reference to deletion of data already acquired by the data fiduciary in this section. Additionally, the right to restrict or prevent continuing disclosure of personal data applies only where the data protection authority, through an adjudicating officer (appointed under section 68), determines that any of the grounds listed above for the restriction or prevention of disclosure of personal data exist.

■ Right to object to processing

Rule 5 of the IT Rules states that the data subject or provider of information shall have the option to later withdraw consent which may have been given to the corporate entity previously; such withdrawal of consent must be stated in writing to the body corporate. On withdrawal of consent, the body corporate is prohibited from processing the personal information in question.

In the case of the data subject not providing consent, or later withdrawing consent, the body corporate shall have the option not to provide the goods or services for which the information was sought.

■ Right to restrict processing

Please see the information on right to deletion/right to be forgotten above.

■ Right to data portability

The current law contains no specific provisions on the right to data portability. However, section 26 of the PDPB states that the data principal shall have the right to receive data on itself (generated or collected in the course of provision of services or use of goods by the data fiduciary, or which has been provided to the data fiduciary by the data principal, or which forms a part of the profile of the data principal) from the data fiduciary. The data principal also has the right to have such data transferred to another data fiduciary. However, these rights are subject to the condition that such data was processed through automatic means. These rights also do not apply if the processing of such data was necessary for the functions of the State or compliance with the law. Finally, these rights are also vitiating if the disclosure or transfer of such data by the data fiduciary would reveal any trade secrets of the data fiduciary or simply is not technically feasible.

Procedures outlined under section 28 of the PDPB would apply in the enforcement of this right (see answer on the right of access to data, above).

■ Right to withdraw consent

Rule 5 of the IT Rules states that the data subject or provider of information shall have the option to later withdraw consent which may have been given to the corporate entity previously; such withdrawal of consent must be stated in writing to the body corporate. On withdrawal of consent, the body corporate is prohibited from processing the personal information in question.

In the case of the data subject not providing consent, or later withdrawing consent, the body corporate shall have the option not to provide the goods or services for which the information was sought.

■ Right to object to marketing

This is the same as the “objection to processing”; see above.

■ Right to complain to the relevant data protection authority(ies)

Rule 5, subsection 9 of the IT Rules mandates that all discrepancies or grievances reported to data controllers must
What information must be included in the registration/notification? (e.g., per legal entity, per processing purpose, per data category, per system or database)?

The current law does not contain provisions on the registration of entities that process data. However, the PDPB states that the data protection authority (established as envisaged by the PDPB) may notify certain data fiduciaries as “significant data fiduciaries” based on the factors listed in the answer to question 6.1 above. In addition to these factors, the authority may notify significant data fiduciaries based on any other factor it deems relevant in causing harm to the data principals as a consequence of the processing of their data by the fiduciary in question. Similarly, the authority may also require fiduciaries it does not consider significant to nonetheless comply with registration requirements. See the answer to question 6.1 for more information.

Who must register with/notify the data protection authority (e.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation)?

The current law does not contain provisions on the registration of entities that process data. As per the PDPB, should it come into force, who must register with the authority and the procedures for such registrations will be determined by the data protection authority established under the PDPB.

What information must be included in the registration/notification (e.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes)?

Please see the answer to question 6.4.

What are the sanctions for failure to register/notify where required?

Please see the answer to question 6.4. The PDPB specifies in section 69 that when the data fiduciary contravenes registration requirements, it shall be liable to a penalty which may extend to up to either two percent of its total worldwide turnover in the preceding financial year, or INR 50 million, whichever is higher.

What is the fee per registration/notification (if applicable)?

Please see the answer to question 6.4.

How frequently must registrations/notifications be renewed (if applicable)?

Please see the answer to question 6.4.
6.9 Is any prior approval required from the data protection regulator?

Please see the answer to question 6.4.

6.10 Can the registration/notification be completed online?

Please see the answer to question 6.4.

6.11 Is there a publicly available list of completed registrations/notifications?

Please see the answer to question 6.4.

6.12 How long does a typical registration/notification process take?

Please see the answer to question 6.4.

7 Appointment of a Data Protection Officer

7.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.

Neither the IT Act nor the IT Rules mention the appointment or role of a Data Protection Officer.

According to section 46 of the IT Act, an Adjudicating Officer shall be appointed by order of the Central Government for the purpose of discerning whether or not any person has contravened any provision of the IT Act. The Adjudicating Officer has the trappings of a civil court. In addition, section 48 of the Act provides for the establishment – by notification – of an appellate tribunal known as the Cyber Regulations Appellate Tribunal. The tribunal will have an appellate jurisdiction and is entitled to exercise its jurisdiction both on fact and law over a decision or order passed by the Adjudicating Officer or the Controller of Certifying Authorities.

The appointments of both the Adjudicating Officer, as well as the Cyber Regulations Appellate Tribunal, are optional and entirely at the discretion of the Central Government. The Act does not specify which circumstances justify the appointment of the Adjudicating Officer or the Appellate Tribunal. It is also unclear whether such appointment is made suo moto or on representation by another party.

However, should the PDPB come into force, section 36 will require every data fiduciary without exception to appoint a data protection officer to carry out various functions specified by the PDPB, in addition to which the data fiduciary may also specify functions for the officer as necessary.

7.2 What are the sanctions for failing to appoint a Data Protection Officer where required?

The PDPB specifies in section 69 that when the data fiduciary fails to appoint a data protection officer under section 36, it shall be liable to a penalty which may extend up to either two percent of its total worldwide turnover in the preceding financial year, or INR 50 million, whichever is higher.

7.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect of his or her role as a Data Protection Officer?

Neither the current law nor the PDPB provide any specific guidance in this regard. However, section 39 of the PDPB states that if a grievance raised by a data principal before a data protection officer is not resolved within the stipulated time, or if the data principal is not satisfied with the resolution provided, it may file a complaint with the adjudication wing of the data protection authority as prescribed in section 68 of the PDPB. Further appeal lies with the Appellate Tribunal.

7.4 Can a business appoint a single Data Protection Officer to cover multiple entities?

Possibly, see the answer to question 7.1. The PDPB does not address this question but does not expressly forbid such an appointment. It would therefore likely be acceptable unless specified otherwise by the data protection authority established under the PDPB.

7.5 Please describe any specific qualifications for the Data Protection Officer required by law.

Since the law does not address the appointment of a Data Protection Officer specifically, there are no statutorily prescribed qualifications for this position.

However, under section 46 of the IT Act, the Adjudicating Officer must not be below the rank of a Director to the Government of India, or an equivalent officer of the State Government, and must possess such experience in the field of information technology and legal or judicial experience as may be prescribed by the Central Government. If more than one Adjudicating Officer is appointed, the Central Government will determine the jurisdictional powers of the officers.

Under section 48 of the IT Act, the Central Government has been given a mandate to employ more than one Cyber Regulations Appellate Tribunal, but the language of Rule 13 of the Cyber Regulations Tribunal (Procedure) Rules (2000) makes it clear that there shall be only one tribunal. The tribunal must consist of one person only, referred to in section 49 of the Act as the Presiding Officer of the Cyber Appellate Tribunal. The qualifications of the Presiding Officer must be the following:

1. that he is, or has been, or is qualified to be, a Judge of the High Court; or
2. he is or has been a member of the Indian Legal Service and is holding or has held a post in Grade 1 of that service for at least three years.

The Central Government has not so far appointed a Presiding Officer for the Cyber Regulations Appellate Tribunal. See also question 7.1 above.

The PDPB does not provide for eligibility criteria, but under section 108, the data protection authority has the power to make regulations specifying the eligibility and qualification requirements for a data protection officer.

7.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?

Section 46 of the IT Act mandates that an Adjudicating Officer is
appointed by the Central Government for the purposes of holding an inquiry in the manner prescribed by the Central Government. This section further states that the Adjudicating Officer shall, after giving the person who has committed the alleged contravention a reasonable opportunity for making representation in the matter, and if, on such inquiry, he is satisfied that the person has committed the contravention, may impose such penalty or award such compensation as he thinks fit in accordance with the provisions of that section.

Section 47 of the Act states that the factors to be taken into account by the Adjudicating Officer in determining the quantum of compensation are the following:

(a) the amount of gain of unfair advantage, wherever quantifiable, made as a result of the default; and
(b) the amount of loss caused to any person as a result of the default and the repetitive nature of the default.

The Cyber Regulations Appellate Tribunal, being an appellate body, has the power to examine the correctness, legality or propriety of the decision or order passed by the Controller of Certifying Authorities or the Adjudicating Officer under the IT Act. This power is absolute; which, by implication, bars the jurisdiction of civil courts to hear such appeals.

The Act grants an unconditional right of appeal to any aggrieved party to appeal an order made by the Controller or an Adjudicating Officer under this Act. Further, the appeal before the Tribunal shall be filed within a period of 45 days from the date on which a copy of the order made by the Controller or the Adjudicating Officer is received by the person so aggrieved, according to section 57 of the Act. The judicial function of the Cyber Regulations Appellate Tribunal is to give the parties to the appeal an opportunity to be heard, and to pass such orders thereon as it thinks fit, confirming, modifying or setting aside the order appealed against.

Under section 57, subsection 6 of the Act, the emphasis is on employing all ‘judicial means’ to dispose of the appeal within six months of the date of receipt of the appeal. The Act further provides a second forum of appeal in the form of the High Court (the first being the Cyber Regulations Appellate Tribunal) to any person aggrieved by any decision or order of the Cyber Regulations Appellate Tribunal. An appeal is to be filed within 60 days from the date of communication of the decision or order of the Cyber Regulations Appellate Tribunal, on any question of fact or law arising out of said order.

The PDPB enumerates the functions of the data protection officer in section 36 as follows:

“(a) providing information and advice to the data fiduciary on matters relating to fulfilling its obligations under this Act;
(b) monitoring personal data processing activities of the data fiduciary to ensure that such processing does not violate the provisions of this Act;
(c) providing advice to the data fiduciary where required on the manner in which data protection impact assessments must be carried out, and carry out the review of such assessment as under sub-section (4) of section 33;
(d) providing advice to the data fiduciary, where required on the manner in which internal mechanisms may be developed in order to satisfy the principles set out under section 29;
(e) providing assistance to and cooperating with the Authority on matters of compliance of the data fiduciary with provisions under this Act;
(f) act as the point of contact for the data principal for the purpose of raising grievances to the data fiduciary pursuant to section 39 of this Act; and
(g) maintaining an inventory of all records maintained by the data fiduciary pursuant to section 34.”

Section 36 also states that the data fiduciary may assign additional functions to the data protection officer, should it consider it necessary to do so.

7.7 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?

The IT Act and IT Rules do not address the question of registration/ notification of appointment of a Data Protection Officer to the relevant data protection authority(ies). The PDPB also does not address this question. Presumably, however, the data protection authority established under the PDPB will have the power to require such registration and specify exact procedures in this regard.

7.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?

The IT Act and Rules are silent in this regard. However, the PDPB does state in section 8 that the data fiduciary shall provide the data principal with the identity and contact details of the data protection officer no later than at the time of collection of the personal data or, if the data is not collected from the data principal, as soon as is reasonably practicable.

8 Appointment of Processors

8.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?

Neither the IT Act nor the IT Rules address this.

However, the PDPB states in section 15, when defining “data processor”, that it applies to any person, including the State, a company, any juristic entity or any individual who processes personal data on behalf of a data fiduciary. Regardless of the existence of an agreement between a data fiduciary and the data processor, the obligations under the PDPB, should it come into force, would apply to a data processor in full. Further, section 37 of the PDPB states the following:

“(1) The data fiduciary shall only engage, appoint, use or involve a data processor to process personal data on its behalf through a valid contract.

(2) The data processor referred to in sub-section (1) shall not further engage, appoint, use, or involve another data processor in the relevant processing on its behalf except with the authorisation of the data fiduciary, unless permitted through the contract referred to in sub-section (1).

(3) The data processor, and any employee of the data fiduciary or the data processor, shall only process personal data in accordance with the instructions of the data fiduciary unless they are required to do otherwise under law and shall treat any personal data that comes within their knowledge as confidential.”

8.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?

As mentioned above, this issue has not been addressed by the
9 Marketing

9.1 Please describe any legislative restrictions on the sending of electronic direct marketing (e.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?).

There are no legislative guidelines or statutory regulations governing marketing communications through email or text. However, the Telecom Unsolicited Commercial Communications Regulations (2007) and the Telecom Commercial Communications Customer Preference Regulations (2010), both made under the Telecom Regulatory Authority of India (TRAI) 1997, regulate unsolicited commercial communications through telephone or by text. The Regulations state that telemarketers must register themselves with TRAI before they may send out marketing communication through telephone or text messages.

The Regulations also provide for those who wish not to receive unsolicited commercial communication to opt out of receiving said telephone calls or text messages. This is done simply by registering one’s preference with the Customer Preference Registration Facility, which is statutorily required to be set up by the local access provider (defined in the Regulations as including the basic telephone service provider, the cellular mobile telephone service provider and the unified access service provider) or by registering with the National Do Not Call Register.

The PDPB does not talk about electronic direct marketing generally. However, it does provide in section 23 that the data protection authority shall notify as “guardian data fiduciaries” any “data fiduciaries who operate commercial websites or online services directed at children”, or “data fiduciaries who process large volumes of personal data of children”. The PDPB further states that “guardian data fiduciaries shall be barred from profiling, tracking, or behavioural monitoring of, or targeted advertising directed at children”.

The proposed Privacy Bill, 2011, in Chapter VI, section 30, places restrictions on direct marketing. When the Bill is enacted, no person shall be permitted to hold or process a personal database used for direct marketing services, unless he is registered with the National Data Registry and one of the purposes of registration is in fact direct marketing, he has a record stating the source from which he obtained the personal data, and all the individuals whose data are contained in the database have consented to receive direct marketing communication from the person in question.

9.2 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.).

Please see the answer to question 9.1.

9.3 Do the restrictions noted above apply to marketing sent from other jurisdictions?

Neither the IT Act and IT Rules nor the PDPB address this.

9.4 Is/are the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?

Telemarketers may apply to Access Providers for telemarketing resources only after they have registered with TRAI. If telemarketers continue to send unsolicited commercial communication to telephone and mobile numbers who have registered themselves with the National Do Not Call Register or have opted out of receiving said communication with the Customer Preference Registration Facility, complaints may be made, toll-free, to the Access Provider, who then serves a notice upon the telemarketer in breach. Chapter III, Regulation 18 of the Telecom Commercial Communications Customer Preference Regulations (2010) provides for the blacklisting of telemarketers who have received said notice six times or more. No Access Provider is permitted to provide telecom resources to said telemarketer.

9.5 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?

Neither current nor proposed legislation contains provisions on this.

9.6 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?

Please see the answer to question 9.4.

10 Cookies

10.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).

Due to the fact that India has no comprehensive data protection regime, issues such as cookie consent have not so far been addressed by Indian legislation.

10.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?

Please see the answer to question 10.1.

10.3 To date, has/have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?

No; please see the answer to question 10.1.

10.4 What are the maximum penalties for breaches of applicable cookie restrictions?

Please see the answer to question 10.1.
11 Restrictions on International Data Transfers

11.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.

Section 7 of the IT Rules states that bodies corporate can transfer sensitive personal data to any other body corporate or person within or outside India, provided that the transferee ensures the same level of data protection which the body corporate has maintained, as required by the IT Rules. A data transfer is only allowed if either:
1. it is required for the performance of a lawful contract between the data controller and the data subjects; or
2. the data subjects have consented to the transfer.

Should the PDPB come into force, it will apply more stringent restrictions on cross-border transfers of personal data. Section 40 lists the following:

“(1) Every data fiduciary shall ensure the storage, on a server or data centre located in India, of at least one serving copy of personal data to which this Act applies.

(2) The Central Government shall notify categories of personal data as critical personal data that shall only be processed in a server or data centre located in India.

(3) Notwithstanding anything contained in sub-section (1), the Central Government may notify certain categories of personal data as exempt from the requirement under subsection (1) on the grounds of necessity or strategic interests of the State.

(4) Nothing contained in sub-section (3) shall apply to sensitive personal data.”

11.2 Please describe the mechanisms businesses typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).

In a “Press Note” released on August 24, 2011, the Ministry of Information Technology clarified that the rules on sensitive data transfer described above are limited in jurisdiction to Indian bodies corporate and legal entities or persons, and do not apply to bodies corporate or legal entities abroad. As such, information technology industries and business process outsourcing companies ascribe to secure methods of data transfer which they prefer, provided that the transfer in question does not violate any law either in India or in the country to which the data is being transferred.

In section 41, the PDPB lists the following conditions for cross-border transfer of personal data:

“(1) Personal data other than those categories of sensitive personal data notified under subsection (2) of section 40 may be transferred outside the territory of India where—
(a) the transfer is made subject to standard contractual clauses or intra-group schemes that have been approved by the Authority; or
(b) the Central Government, after consultation with the Authority, has prescribed that transfers to a particular country, or to a sector within a country or to a particular international organisation is permissible; or
(c) the Authority approves a particular transfer or set of transfers as permissible due to a situation of necessity; or
(d) in addition to clause (a) or (b) being satisfied, the data principal has consented to such transfer of personal data; or
(e) in addition to clause (a) or (b) being satisfied, the data principal has explicitly consented to such transfer of sensitive personal data, which does not include the categories of sensitive personal data notified under sub-section (2) of section 40.

(2) The Central Government may only prescribe the permissibility of transfers under clause (b) of sub-section (1) where it finds that the relevant personal data shall be subject to an adequate level of protection, with regard to the applicable laws and international agreements, and the effectiveness of the enforcement by authorities with appropriate jurisdiction, and shall monitor the circumstances applicable to such data in order to review decisions made under this sub-section.

(3) Notwithstanding sub-section (2) of Section 40, sensitive personal data notified by the Central Government may be transferred outside the territory of India—
(a) to a particular person or entity engaged in the provision of health services or emergency services where such transfer is strictly necessary for prompt action under section 16; and
(b) to a particular country, a prescribed sector within a country or to a particular international organisation that has been prescribed under clause (b) of sub-section (1), where the Central Government is satisfied that such transfer or class of transfers is necessary for any class of data fiduciaries or data principals and does not hamper the effective enforcement of this Act.

(4) Any transfer under clause (a) of sub-section (3) shall be notified to the Authority within such time period as may be prescribed.

(5) The Authority may only approve standard contractual clauses or intra-group schemes under clause (a) of sub-section (1) where such clauses or schemes effectively protect the rights of data principals under this Act, including in relation with further transfers from the transferees of personal data under this sub-section to any other person or entity.

(6) Where a data fiduciary seeks to transfer personal data subject to standard contractual clauses or intra-group schemes under clause (a) of sub-section (1), it shall certify and periodically report to the Authority as may be specified, that the transfer is made under a contract that adheres to such standard contractual clauses or intra-group schemes and that it shall bear any liability for the harm caused due to any non-compliance with the standard contractual clauses or intra-group schemes by the transferee.”

11.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.

The current legislation does not contain provisions addressing this issue, but for the PDPB provisions, please see the answers to questions 11.1 and 11.2.

12 Whistle-blower Hotlines

12.1 What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?

The Whistle Blowers Protection Act, 2011 mandates that any public
servant, or any person including any non-governmental organisation, may make a public interest disclosure before the Competent Authority. Section 4(6) of the Act states that no action shall be taken if the disclosure does not indicate the identity of the complainant. Section 6 mandates that the Competent Authority shall not take notice of any disclosure which relates to a matter or issue determined by a Court or Tribunal, to the extent that the disclosure seeks to reopen such matter or issue. It also mandates that the Competent Authority shall not investigate any disclosure involving an allegation if the complaint is made after the expiry of seven years from the date on which the action complained against is alleged to have taken place. Section 8 of the Act exempts matters related to the sovereignty, security and integrity of India, matters which may affect friendly relations with a foreign state, public order, decency or morality or in relation to contempt of court, defamation or incitement to an offence pertaining to the disclosure of proceedings of the Cabinet of the Union and State Government or any committee of the Cabinet from disclosure.

An amendment was proposed and passed by the Parliament to the Act. It seeks to further exempt: (a) information, the disclosure of which would cause a breach of parliamentary privilege; (b) information relating to commercial confidence, trade secrets or intellectual property, the disclosure of which would harm the competitive position of a third party, unless such information has been disclosed to the complaint under the Right to Information Act; (c) information which is available to a person in his fiduciary capacity; (d) information received in confidence from a foreign government; (e) information, disclosure of which would endanger the life or physical safety of a person or identify the source of information; and (f) information which would impede the process of investigation or apprehension or prosecution of offenders from disclosure. The amendment is yet to receive the assent of the President and be promulgated into law.

The PDPB does not address whistle-blowing, except insofar as to say in section 17 that the data protection authority it envisages may prescribe it as a reasonable purpose for the processing of personal data.

12.2 Is anonymous reporting prohibited, strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do businesses typically address this issue?

See the answer to question 12.1 above. There have been no reported instances where companies have had to address the issue of anonymous reporting.

13 CCTV

13.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?

Current legislation does not touch upon questions relating to CCTV surveillance. However, the Privacy Bill, 2011, did state in Chapter V, section 26 that the installation and operation of CCTV surveillance in public areas shall be in accordance with prescribed procedure for legitimate and proportionate objectives and will not affect his right to privacy. There are no registration requirements specifically laid out in this proposed legislation, neither does it elaborate on what the prescribed procedure for the installation and operation of CCTV will be.

13.2 Are there limits on the purposes for which CCTV data may be used?

Current legislation does not touch upon questions relating to CCTV surveillance. However, the Data Privacy Bill, 2017 provides that, apart from reasonable restrictions such as safeguarding the national security or defence of India, prevention of acts of terrorism, corruption, money laundering, organised crime, sale or purchase of narcotic and psychotropic substances, investigation of cognisable offences and maintenance of public order, no person shall conduct or assist in conducting any surveillance. Targeted profiling of individuals or of a certain section or class of persons without any basis is expressly barred. The onus to prove that information or personal data obtained through surveillance was so done while maintaining a proper chain of custody without any tampering or external interference, in a court of law, shall be on the concerned state authority, intelligence or private entity, as the case may be.
15 Data Security and Data Breach

15.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?

Rule 8 of the IT Rules describes reasonable security practices and procedures as follows:

1) A body corporate, or a person on its behalf, shall be considered to have complied with reasonable security practices and procedures if they have implemented such security practices and standards, have a comprehensive documented information security programme and information security policies that contain managerial, technical, operational and physical security control measures that are commensurate with the information assets being protected and with the nature of the business in question.

2) In the event of an information security breach, the body corporate or a person on its behalf shall be required to demonstrate, as and when called upon to do so by the agency mandated under the law, that they have implemented security control measures as per their documented information security programme and information security policies. The international standard IS/ISO/IEC 27001 on “Information Technology − Security Techniques − Information Security Management System − Requirements” is one such standard.

3) Any industry association or an entity whose members are self-regulating by following codes other than the IS/ISO/IEC codes of best practice for data protection as per (1) above, shall get its codes of best practice duly approved and notified by the Central Government. The body corporate or a person on its behalf, that has implemented either the IS/ISO/IEC 27001 standard or the codes of best practice for data protection as approved and notified under point (3) above, shall be deemed to have complied with reasonable security practices and procedures, provided that such a standard or such codes of best practice are certified or audited on a regular basis by an independent auditor, duly approved by the Central Government. This audit shall be carried out by an auditor at least once a year, or as and when the body corporate undertakes a significant upgrade of its process and computer resources.

In August 2011, the Ministry of Communications and Information issued a “Press Note” (Clarification on the Privacy Rules) which provides that any Indian outsourcing service provider/organisation providing services relating to collection, storage, dealing or handling of sensitive personal information or personal information under contractual obligations with a legal entity located within or outside India is not subject to collection and disclosure of information requirements, or consent requirement as detailed by the IT Rules, provided it does not have direct contact with the data subjects when providing their services.

In section 4, the PDPB specifies that any person processing personal data owes a duty to the data principal to process such personal data in a fair and reasonable manner that respects the privacy of the data principal. Sections 5 to 11 contain provisions on accountability, data storage limitation, data quality, notice to data principals, lawful processing, collection limitation and purpose limitation. The PDPB also prescribes the establishment of a data protection authority which is empowered to create further regulations in this regard. In section 31, the PDPB prescribes certain security safeguards as follows:

“(1) Having regard to the nature, scope and purpose of processing personal data undertaken, the risks associated with such processing, and the likelihood and severity of the harm that may result from such processing, the data fiduciary and the data processor shall implement appropriate security safeguards including:

(a) use of methods such as de-identification and encryption;
(b) steps necessary to protect the integrity of personal data; and
(c) steps necessary to prevent misuse, unauthorised access to, modification, disclosure or destruction of personal data.

(2) Every data fiduciary and data processor shall undertake a review of its security safeguards periodically as may be specified and may take appropriate measures accordingly.”

15.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

The current legislation does not contain any provisions that address this. However, the PDPB states the following in section 32:

“(1) The data fiduciary shall notify the Authority of any personal data breach relating to any personal data processed by the data fiduciary where such breach is likely to cause harm to any data principal.

(2) The notification referred to in sub-section (1) shall include the following particulars—

(a) nature of personal data which is the subject matter of the breach;
(b) number of data principals affected by the breach;
(c) possible consequences of the breach; and
(d) measures being taken by the data fiduciary to remedy the breach.

(3) The notification referred to in sub-section (1) shall be made by the data fiduciary to the Authority as soon as possible and not later than the time period specified by the Authority, following the breach after accounting for any time that may be required to adopt any urgent measures to remedy the breach or mitigate any immediate harm.

(4) Where it is not possible to provide all the information as set out in sub-section (2) at the same time, the data fiduciary shall provide such information to the Authority in phases without undue delay.

(5) Upon receipt of notification, the Authority shall determine whether such breach should be reported by the data fiduciary to the data principal, taking into account the severity of the harm that may be caused to such data principal or whether some action is required on the part of the data principal to mitigate such harm.

(6) The Authority, may in addition to requiring the data fiduciary to report the personal data breach to the data principal under sub-section (5), direct the data fiduciary to take appropriate remedial action as soon as possible and to conspicuously post the details of the personal data breach on its website.

(7) The Authority may, in addition, also post the details of the personal data breach on its own website.”
15.3 Is there a legal requirement to report data breaches to affected data subjects? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

Not in the current law. However, for information on the provisions of the PDPB addressing this issue, refer to the answer to question 15.2.

15.4 What are the maximum penalties for data security breaches?

There are no specific penalties in the current legislation. However, the PDPB states in section 69 that for failing to take prompt and appropriate action in response to a data security breach, the data fiduciary shall be liable to a penalty which may extend to up to either two percent of its total worldwide turnover in the preceding financial year, or INR 50 million, whichever is higher. Further, for contravening any of the provisions in the PDPB on lawful, fair and reasonable processing of personal data or sensitive personal data, the data fiduciary shall be liable to a penalty which may extend up to INR 150 million or four percent of its total worldwide turnover of the preceding financial year, whichever is higher.

16. Enforcement and Sanctions

16.1 Describe the enforcement powers of the data protection authority(ies).

The current law does not provide for a special data protection authority. All enforcement of existing laws is carried out directly by courts or specialised tribunals as mentioned in various answers above. However, the PDPB does envisage the establishment of a data protection authority in section 49 and lists the powers and functions of such an authority in section 60. In general, the duty of the authority would be “to protect the interests of data principals, prevent any misuse of personal data, ensure compliance with the provisions of the PDPB and to promote awareness of data protection”.

16.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?

As previously mentioned, there is no data protection authority currently in force. However, one may be established if the PDPB comes into effect. Such an authority would have the power to regulate and specify reasonable purposes for which personal data may be processed and to that extent could prevent the processing of personal data should it deem the purpose for such processing unreasonable.

16.3 Describe the data protection authority’s approach to exercising those powers, with examples of recent cases.

Please see the answers to questions 16.1 and 16.2.

16.4 Does the data protection authority ever exercise its powers against businesses established in other jurisdictions?

Please see the answers to questions 16.1 and 16.2, and in addition the answers to questions 11.1 and 11.2.

17 E-discovery / Disclosure to Foreign Law Enforcement Agencies

17.1 How do businesses typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?

As long as requests from foreign companies are based on an order from a court of law and if the country in question has a reciprocal arrangement with India, then such a request may be enforced in India, if necessary, through an Indian court. Absent a court order, Indian companies do not have any obligation to respond to foreign e-discovery requests or requests for disclosure.

17.2 What guidance has/have the data protection authority(ies) issued?

None. Please refer to section 16 above.

18 Trends and Developments

18.1 What enforcement trends have emerged during the previous 12 months? Describe any relevant case law.

India is seeing a definite increase in executive, legislative and judicial interest in bolstering our legal framework in data protection and privacy. The Supreme Court handed down a landmark judgment on privacy and the public interest in September 2018. In a case entitled Justice K.S. Paitaswaray (ret’d.) and Another v. Union of India and Others Writ Petition (Civil) No 494 of 2012, the Supreme Court recognised the importance of developing a new data protection regime and placed limitations and restrictions on the collection and retention of personal data of Indian citizens by the government under The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016. This decision also issued directions for the establishment of the ten-member committee of experts referred to in Section 1 above, leading to an extensive White Paper followed by a detailed report and draft legislation for new data protection laws in India.

18.2 What “hot topics” are currently a focus for the data protection regulator?

Subsequent to the passage of the General Data Protection Regulation in Europe and in view of the imminent change in Indian data protection laws, all stakeholders in India are scrambling to examine methods of collection and retention of personal data, privacy policies and the issue of consent. As mentioned in the answer to question 1.1, the PDPB is likely to be tabled before Parliament shortly. Should it pass into law, it will make these issues and others very real areas of concern for regulators and processors alike.
Hari Subramaniam is an attorney-at-law with a background in medical sciences. He is the Managing Partner of one of the leading New Delhi-based law firms specialised in intellectual property rights (IPR), Subramaniam & Associates (SNA). He has been in practice in the field of patents and trademarks for 35 years and has been involved in several important IPR and contentious cases in India and abroad. He has one of the best track records in Patent Oppositions in India. He is a major contributor to, and speaker at, various workshops on intellectual property laws conducted worldwide, including: the World Intellectual Property Organization; leading universities around the world; the Intellectual Property Owners’ Association, USA; the American Bar Association; Judicial Academies; the Indo-Pacific Juristic Forum; the International Association for the Protection of Intellectual Property; the Asian Patent Attorneys Association; the American Intellectual Property Law Association; and various Patent Offices. Mr. Subramaniam has authored several articles on patents and is on the teaching faculties of several institutions, such as: the Indian Law Institute, New Delhi; the Faculty of Law, New Delhi; and the Academy of Intellectual Property Laws, Mumbai. He has been an expert witness before the Parliament for the amendment of patent laws. He was a member of the three-member team invited by the Mauritius Research Council, headed by the Prime Minister of Mauritius, to advise it on Patent Law amendments in August 2002. He has been recognised as a top-tier attorney by IAMs, Managing Intellectual Property, The Legal 500 Asia Pacific, Asia Law, etc., and has also won the ‘Leading IP Lawyer of the Year’ award several times. He is a member of several international organisations connected with Intellectual Property and is the President of the Asian Patents Attorneys Association, India Chapter. He featured in Asia Law’s “50 Leading IP Lawyers one must know in Asia and Asia Pacific”.

Aditi Subramaniam has a Bachelor’s degree in Law from the University of Oxford and a Master’s degree in Law from Columbia Law School. She is qualified to practise law in India and has recently passed the New York Bar Examination. She specialises in patent and trademark procurement and contentious matters, including oppositions and appeals before the Intellectual Property Office and the Appellate Board, as well as litigation before the District and High Courts. She also advises clients on data protection, pharmaceutical advertising and cyber security. She is widely published and very well regarded in the Indian and international legal fraternity.

Subramaniam & Associates (SNA) is a full-service IP firm with 26 highly qualified attorneys. It boasts a very impressive list of clients and represents several Fortune 500 companies, leading corporations, universities and law firms from all over the world. It also represents a large number of domestic corporations worldwide. The firm is equipped to provide complete and highly cost-effective services, from drafting, filing and prosecution of applications to searches, oppositions and enforcement. It has an excellent network of associates and correspondent counsels worldwide. SNA is one of the largest filers of PCT International Applications from India and is regarded by the Indian Patent Office and the industry as a top IP firm in India. SNA provides its clients with a personalised service – professional in approach and reliable irrespective of any time constraints. It possesses the latest technology and sophisticated software to enable its attorneys to keep track of all critical deadlines. The work systems are adapted to meet the specific needs of each client.

SNA's team of attorneys includes specialists in different technical fields as well as in litigation. SNA's clients are assured of easy access to appropriate advice at different stages in the creation, filing, prosecution, protection, management, exploitation and enforcement of their intellectual property.

With representation in major cities of India, such as Calcutta, Chennai and Mumbai, and long-established relationships with local counsel throughout the world, SNA is well-positioned to serve its clients’ domestic and international needs.
1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

Personal data protection of Indonesian residents is regulated on a sectoral basis (see question 1.3). There is no single principal data protection legislation in Indonesia.

1.2 Is there any other general legislation that impacts data protection?

The Indonesian Constitution confers to individuals certain basic human rights, including right to privacy and right to protection of his/her properties. These two rights are fundamentally the tenets for personal data protection in Indonesia.

Law No. 11 of 2008 on Electronic Information and Transaction Law (as amended) (EIT Law) requires a party that operates an electronic system to, among others, put in place certain security measures to prevent any failure or disturbance to the electronic systems (including any transactions utilising, or taking place within, the electronic system that involves personal data). These measures can include anti-virus software, anti-spamming software, firewall and intrusion detection.

1.3 Is there any sector-specific legislation that impacts data protection?

Some of the key sector-specific pieces of legislation are as follows:

- Personal data related to banking is governed under the framework and implementing regulations of Law No. 7 of 1992 on Banking, as amended by Law No. 10 of 1998 and Bank Indonesia Regulation No. 16/1/PBI/2014 on Protection of Consumers of Payment System Services, which contain provisions related to bank secrecy, banking information requests made by law enforcement agencies, and obligation of banking service providers to secure consent of the relevant individual before disclosing his/her personal data to third parties.

- Personal data related to financial services is regulated by the Financial Services Authority, among others under the Financial Services Authority Regulation No. 1/POJK.07/2013 on Consumer Protection in the Financial Services Sector (as amended) (Financial Services Consumer Protection Regulation) and Financial Services Authority Circular Letter No. 14/SEOJK.07/2014 on Confidentiality and Security of Personal Information and/or Data of Consumers (Financial Services Consumer Protection Letter), which requires financial service providers to secure prior consent in order to contact customers directly and to disclose their personal data to third parties.

- Personal data related to telecommunications is governed under the framework and implementing regulations of Law No. 36 of 1999 on Telecommunications and Government Regulation No. 52 of 2000 on Telecommunication Operations, which requires telecommunication operators, both service and network providers, to maintain the confidentiality of the information sent and received by their customers through their services or networks.

- Personal data related to citizen administration is governed under the framework and implementing regulations of Law No. 23 of 2006 on Citizen Administration, as amended by Law No. 24 of 2013, and Government Regulation No. 37 of 2007 on Implementation of Law No. 23 of 2006 on Citizen Administration, as amended by Government Regulation No. 102 of 2012, which requires government authorities and officials to maintain the confidentiality of the personal data of Indonesian nationals.

- Personal data related to health is governed under the framework and implementing regulations of Law No. 36 of 2009 on Health, Government Regulation No. 46 of 2014 on Health Information Systems, and Minister of Health Regulation No. 269/MENKES/PER/III/2008 on Medical Records, which regulate the confidentiality of health information and medical records of individuals (except under specific circumstances) and restrictions on collecting, processing, and storing of health data and information (for example, health data and information must be stored locally).

- Personal data collected, processed, stored, transferred and/or destroyed using electronic systems are regulated under the Minister of Communication and Information Technology Regulation No. 20 of 2016 on Personal Data Protection in Electronic Systems (PDP Regulation). The PDP Regulation is currently the most comprehensive sector-specific legislation that governs the processing of personal data.

1.4 What authority(ies) are responsible for data protection?

There is no dedicated data protection authority in Indonesia. The authority responsible for data protection would depend on the sector. For example, (i) the Ministry of Communication and Information Technology is responsible for electronic personal data and telecommunication data; (ii) the Ministry of Health is responsible for personal data related to health; (iii) the Ministry of Internal Affairs is responsible for citizen administration data; and
(iv) the Financial Services Authority is responsible for personal data in the financial services and banking sectors.

2 Definitions

2.1 Please provide the key definitions used in the relevant legislation:

- **“Personal Data”**
  Personal Data is defined as “certain data of an individual which are stored, maintained and kept accurate, and its confidentiality is protected”, while certain data of an individual is “every accurate and factual information which is, either directly or indirectly, inherent in and identifiable to each person, and the use of which shall be in accordance with the provisions of statutory laws and regulations”.

- **Processing**
  The current legislation does not provide any definition of “processing”.

- **Controller**
  The current legislation does not provide any definition of “controller”.

- **Processor**
  The current legislation does not provide any definition of “processor”.

- **Data Subject**
  Data Subject is defined as “the individual to whom the Certain Data of an Individual belongs to”.

- **Sensitive Personal Data**
  The current legislation does not provide any definition of “sensitive personal data”.

- **Data Breach**
  The current legislation does not provide any definition of “data breach”.

Other key definitions – please specify (e.g., “Pseudonymous Data”, “Direct Personal Data”, “Indirect Personal Data”)

1. Electronic system providers are defined as “any person, State authority, business entity or community that provides, manages, and/or operates an electronic system, whether independently or jointly, in the interest of the electronic system’s users and/or the interests of other parties”.

2. Electronic system is defined as “a set of electronic devices and procedures used for the purpose of preparing, collating, processing, analysing, storing, displaying, and disseminating electronic data”.

3. Electronic data is defined as “text, sounds, images, maps, drafts, photographs, electronic data interchange (EDI), electronic mails, telegrams, telex, telecopy or the like, letters, signs, figures, access codes, symbols, or perforations that have been processed or understandable to persons qualified to understand them”.

3 Territorial Scope

3.1 Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to those laws?

The EIT Law applies not only to activities carried out within Indonesia, but also to activities carried out abroad that has any consequential impact to Indonesia. These impacts may relate to the national economy, defense and security, national sovereignty, and Indonesian nationals and legal entities. As the PDP Regulation is an implementing regulation of the EIT Law, the PDP Regulation also has extraterritorial applicability. Therefore, any collection and processing of personal data of an Indonesian resident by an electronic systems provider based outside of Indonesia will be subject to the PDP Regulation.

4 Key Principles

4.1 What are the key principles that apply to the processing of personal data?

- **Transparency**
  Electronic system providers must inform a data subject of the purposes for the collection, processing and transfer of his/her personal data and make available its contact information to the public if the data subject wishes to access his/her personal data that are kept by the electronic system providers.

- **Lawful basis for processing**
  Processing of personal data must be based on consent from the individuals in question.

- **Purpose limitation**
  An electronic system provider can only use the personal data collected by it from a data subject for purposes that have been informed to such data subject.

- **Data minimisation**
  This principle is not recognised under the current legislation.

- **Proportionality**
  This principle is not recognised under the current legislation.

- **Retention**
  Personal data may only be retained until such time when they are no longer required. Pursuant to the PDP Regulation, if there are no laws or regulations that specifically govern the retention period, the minimal retention period for personal data is five years.

Other key principles – please specify

There are no other key principles for the processing of personal data.

5 Individual Rights

5.1 What are the key rights that individuals have in relation to the processing of their personal data?

- **Right of access to data/copies of data**
  Individuals have the right to access the history of any personal data given by him/her.

- **Right to rectification of errors**
  Individuals have the right to access or be provided with the opportunity to correct his/her personal data.

- **Right to deletion/right to be forgotten**
  Individuals have the right to request the deletion of their personal data. Also, individuals have the ‘right to be forgotten’, i.e., request any irrelevant personal data be deleted. The request ‘to be forgotten’, however, must be based on a court order.

- **Right to object to processing**
  This is not applicable.
Right to restrict processing
Individuals may determine certain personal data to be confidential, which means that such personal data must not be disclosed to any third party.

Right to data portability
This is not applicable.

Right to withdraw consent
This right is not explicitly provided, but the current legislation does not restrict the withdrawal of consent that has been given.

Right to object to marketing
The PDP Regulation does not explicitly stipulate the right to object to marketing, except in the financial services sector as provided under the Financial Services Consumer Protection Regulation and Financial Services Consumer Protection Letter.

Right to complain to the relevant data protection authority(ies)
If an electronic system provider fails to notify any data breach to the data subject or fails to notify as such on a timely manner (within 14 days as of the discovery of such data breach), the affected data subject may file a complaint to the Ministry of Communication and Information Technology.

Other key rights – please specify
A data subject that suffers losses as a result of the failure by an electronic system provider to notify a data breach may file a civil lawsuit against such electronic system provider.

6 Registration Formalities and Prior Approval

6.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?
Under the PDP Regulation, there is no legal obligation for businesses to register with or notify the data protection authority or any other governmental body in respect of its processing activities, except for cross-border personal data transfer as discussed in Section 11.

6.2 If such registration/ notification is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?
This is not applicable.

6.3 On what basis are registrations/notifications made (e.g., per legal entity, per processing purpose, per data category, per system or database)?
This is not applicable.

6.4 Who must register with/notify the data protection authority (e.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation)?
This is not applicable.

6.5 What information must be included in the registration/ notification (e.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes)?
This is not applicable.

6.6 What are the sanctions for failure to register/notify where required?
This is not applicable.

6.7 What is the fee per registration/ notification (if applicable)?
This is not applicable.

6.8 How frequently must registrations/notifications be renewed (if applicable)?
This is not applicable.

6.9 Is any prior approval required from the data protection regulator?
This is not applicable.

6.10 Can the registration/ notification be completed online?
This is not applicable.

6.11 Is there a publicly available list of completed registrations/notifications?
This is not applicable.

6.12 How long does a typical registration/ notification process take?
This is not applicable.

7 Appointment of a Data Protection Officer

7.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.
The function of a Data Protection Officer is not yet recognised under the applicable Indonesian personal data protection legislation. However, the PDP Regulation requires an electronic systems provider that processes personal data to make available a contact person for any inquiry by data subjects regarding matters pertaining to their personal data.

7.2 What are the sanctions for failing to appoint a Data Protection Officer where required?
This is not applicable.
7.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect of his or her role as a Data Protection Officer?

This is not applicable.

7.4 Can a business appoint a single Data Protection Officer to cover multiple entities?

This is not applicable.

7.5 Please describe any specific qualifications for the Data Protection Officer required by law.

This is not applicable.

7.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?

This is not applicable.

7.7 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?

This is not applicable.

7.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?

With regard to the contact person as mentioned in question 7.1 above, the PDP Regulation does not specify where the said person’s contact details must be disclosed. The PDP Regulation only stipulates that the contact person must be easily contactable.

8 Appointment of Processors

8.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?

The applicable Indonesian data protection legislation does not specifically require an agreement to be made when a processor is appointed to process personal data on behalf of another party.

8.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?

This is not applicable.

9 Marketing

9.1 Please describe any legislative restrictions on the sending of electronic direct marketing (e.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?).

Unlike some other jurisdictions where there are Do Not Call provisions under their general personal data protection acts, Indonesian law does not have such provisions under its personal data protection legislation. However, the sending of marketing messages is regulated in certain sectors (e.g., the banking and financial services sectors). Under the banking and financial services sectors’ regulations, service providers can send marketing messages to the customers’ personal lines of communications (e.g., telephone, text message and email) if the customers have given their consent and such messages are delivered at a prescribed period of time (i.e. weekdays and during working hours, unless the customers agree that the message could be delivered to them at any time).

The EIT Law and PDP Regulation will also apply if the marketing message is delivered to the recipient through an electronic system (e.g. email). Based on these pieces of legislation, the party sending the marketing message must obtain the recipient’s consent before using his/her personal data for marketing purposes.

9.2 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.).

See question 9.1 above.

9.3 Do the restrictions noted above apply to marketing sent from other jurisdictions?

The EIT Law and PDP Regulation provisions will apply to any non-Indonesian entity that delivers the marketing message, as these pieces of legislation apply extraterritorially. As such, businesses that intend to send marketing messages using electronic systems from other jurisdictions are subject to the requirements under that legislation (such as the requirement to obtain consent).

9.4 Is/are the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?

Specifically in the banking and financial services sectors, the Financial Services Authority plays an active role in enforcing marketing restriction offences.

9.5 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?

To the extent not restricted by any applicable law and regulations, and by any contractual obligations, purchasing marketing lists from third parties should generally be lawful. However, we understand that in practice sellers of such marketing lists are often suspect (or at least there is reasonable doubt that the list was obtained through legal
9.6 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?

Sanctions for the general failure to comply by sending marketing communications include administrative sanctions in the form of verbal and written warnings, temporary suspension of business activities, and public online disclosure of such non-compliance. Sector-specific sanctions for banking and financial services include fines, restriction and suspension of business activities, and revocation of business licences.

10 Cookies

10.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).

There is no specific regulation that governs the use of cookies.

10.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?

This is not applicable.

10.3 To date, has/have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?

This is not applicable.

10.4 What are the maximum penalties for breaches of applicable cookie restrictions?

This is not applicable.

11 Restrictions on International Data Transfers

11.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.

There is no restriction on the transfer of personal data to another jurisdiction if consent of the data subject has been obtained.

11.2 Please describe the mechanisms businesses typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).

Although not specifically regulated under the applicable Indonesian personal data protection legislation, the mechanism that businesses typically utilise in transferring any personal data abroad includes the execution of a contract that incorporates consent from the data subject to the transfer of their personal data abroad. For example, in the context of a marketplace provider that sends its customers’ personal data abroad, such provider will disclose information about the cross-border transfer in its privacy policy and the customers will need to consent to such policy before using the marketplace platform.

11.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.

The PDP Regulation requires any cross-border personal data transfer to be notified to the Ministry of Communication and Information Technology. This notification must be submitted before the cross-border personal data transfer is conducted and must contain information on the destination country, recipient’s name, intended date of the cross-border personal data transfer, and purpose of the cross-border personal data transfer. In addition, another notification must be submitted after the cross-border personal data transfer is conducted, to elaborate on how it was conducted. Both notices must be submitted physically in a letter addressed to the Minister of Communication and Information Technology.

Currently, the Ministry of Communication and Information Technology has not issued any guidelines regarding the notification. As such, there is no clarity as to the type of cross-border personal data transfer that must be notified.

12 Whistle-blower Hotlines

12.1 What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?

Generally, there is no specific regulation related to corporate whistle-blowing that is applicable to privately owned companies. There is, however, a requirement for state-owned companies to have a whistle-blowing system but without any additional details.
12.2 Is anonymous reporting prohibited, strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do businesses typically address this issue?

As discussed in question 12.1, Indonesian law does not stipulate provisions related to corporate whistle-blowing.

13  CCTV

13.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?

Under the current legislation, the use of CCTV is not regulated. However, based on best practice, when CCTV is used, the responsible party must provide public notice.

13.2 Are there limits on the purposes for which CCTV data may be used?

Under the current legislation, the use of CCTV is not regulated.

14  Employee Monitoring

14.1 What types of employee monitoring are permitted (if any), and in what circumstances?

Any employee monitoring must be based on the consent of the employees concerned.

14.2 Is consent or notice required? Describe how employers typically obtain consent or provide notice.

The employees’ consent is required, and it is usually incorporated into the employment contract or secured through a separate document.

14.3 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?

Labour unions are usually notified or consulted regarding the establishment of business-wide policies related to personal data (such as the establishment of a corporate whistle-blower hotline or the use of employee personal data outside of purposes related to employment).

15  Data Security and Data Breach

15.1 Is there a general obligation to ensure the security of personal data? If so, who are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?

Currently, the applicable Indonesian personal data protection legislation does not differentiate between a controller and a processor. Under the EIT Law and PDP Regulation, the general obligation to ensure the security of personal data lies on an electronic systems provider that processes and stores personal data.

15.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

Under the PDP Regulation, an electronic systems provider that suffers a data breach is not required to notify the incident to the relevant Indonesian regulator and law enforcement agency. However, under Government Regulation No. 82 of 2012 on Application of Electronic Systems and Transactions (Electronic Systems Regulation), if an electronic system suffers a failure (kegagalan) or trouble (gangguan) caused by the action of a third party and such failure or trouble on the electronic system results in serious impact (berdampak serius), the electronic systems provider must notify the relevant Indonesian regulator and law enforcement agency at the earliest possible instance.

15.3 Is there a legal requirement to report data breaches to affected data subjects? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

Under the PDP Regulation, an electronic systems provider that suffers a data breach must notify the affected data subject no later than 14 days as of the discovery of the breach. Such notification must state the reason or cause of the failure and can be delivered electronically if the affected data subject has consented to electronic delivery.

15.4 What are the maximum penalties for data security breaches?

There is no financial penalty for a data breach per se. However, if an electronic systems provider that holds personal data wilfully discloses those data and such disclosure results in the defamation of a data subject, the said provider will be subject to a criminal penalty of a maximum of IDR 750 million and/or imprisonment of up to four years.

16  Enforcement and Sanctions

16.1 Describe the enforcement powers of the data protection authority(ies).

Please refer to our response to question 16.2 below.

16.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?

Indonesia does not have a central data protection authority. The authority to enforce is specified in the relevant laws and regulations. While some laws and regulations include only administrative sanctions (e.g. warnings, suspension), others allow not only...
administrative sanctions, but also enforcement through a private right of action (i.e. tort) by the affected data subject.

16.3 Describe the data protection authority’s approach to exercising those powers, with examples of recent cases.

The data protection authority’s approach would depend on the enforcement mechanism in the relevant law and regulation and the agency conducting the enforcement.

16.4 Does the data protection authority ever exercise its powers against businesses established in other jurisdictions? If so, how is this enforced?

Extraterritorial enforcement of Indonesian laws would depend on a number of factors, including whether the entity is subject to the jurisdiction of the said laws and whether the laws in question have extraterritorial applicability.

17 E-discovery / Disclosure to Foreign Law Enforcement Agencies

17.1 How do businesses typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?

Depending on the foreign e-discovery request or request for disclosure from foreign law enforcement agencies, businesses typically ensure that such foreign law enforcement agency has jurisdiction for such foreign e-discovery request or request for disclosure, and, if necessary, consult with the local law enforcement agency.

17.2 What guidance has/have the data protection authority(ies) issued?

Under the current legislation, there is no guidance on e-discovery or disclosure to foreign law enforcement agencies.

18 Trends and Developments

18.1 What enforcement trends have emerged during the previous 12 months? Describe any relevant case law.

Although not specifically in the area of data protection, the Indonesian regulator (especially the Ministry of Communication and Information Technology) remains active in enforcing the transmission of negative content (e.g. pornographic content, hoaxes, hate speech, etc.).

18.2 What “hot topics” are currently a focus for the data protection regulator?

Since the enactment of the Electronic Systems Regulation, Indonesia has been imposing a data localisation requirement. Essentially, the data localisation requirement requires an electronic system provider that provides “public services” to place their data centre and disaster recovery centre in Indonesia. This would mean that an electronic systems provider will need to store any data that they process in Indonesia.

However, the effects of the data localisation requirement are unclear as there are still uncertainties concerning the definition of “public services”. Given the lack of guidance, multiple electronic systems providers have asked the Indonesian government, through the Ministry of Communication and Information Technology, to clarify this requirement and allow a certain leniency.

As a response, the Ministry of Communication and Information Technology is currently working on a draft amendment of the Electronic Systems Regulation. The draft amendment, among others, no longer requires an electronic systems provider to place its data centre and disaster recovery centre in Indonesia, except if such provider processes and stores “strategic electronic data” (i.e. data that strategically affects the continuity of the country’s administration, defence and security). Nonetheless, there has been no official announcement from the Ministry of Communication and Information Technology on when the amendment will be issued.

The Indonesian government is also working on a draft bill on personal data protection, which is contemplated to become the single principal personal data protection legislation in Indonesia. The bill has been included as part of Indonesia’s 2019 National Priority Legislative Program, which is a list of prioritised legislations that the Parliament will enact in 2019. Based on the latest draft bill on personal data protection that we obtained, it will govern not only the processing of electronic personal data but also physical personal data. It will also regulate the parties that are typically regulated and mentioned in personal data protection legislation, such as the controller and processor.

The draft bill on personal data protection provides criminal sanctions specifically for cases of theft and forgery of personal data. For such cases, individual criminals are subjected to a maximum imprisonment of one year and/or penalty of IDR 300 million, or if the offender is a legal entity, the penalty would be higher, reaching up to IDR 1 billion.

Acknowledgment

The authors would like to thank Andin Aditya Rahman for his contribution to the writing of this chapter. Andin is an Associate at Assegaf Hamzah & Partners, with expertise in the technology, media, and telecommunications sector. He regularly advises on Indonesian laws and regulations issues related to new technologies and business models, such as Internet of Things, artificial intelligence, privacy, big data, cloud computing, blockchain, and over-the-top content, to both domestic and international clients. He has published articles in renowned international publications and is an active member in both local and international organisations, including the Indonesia Cyber Law Community and the Asian Privacy Scholars Network.

Tel: +62 31 5116 4550 ex 110 / Email: andin.rahman@ahp.id
Zacky Zainal Husein
Assegaf Hamzah & Partners
Capital Place, Level 36 & 37
Jalan Jenderal Gatot Subroto Kav. 18
Jakarta 12710
Indonesia
Tel: +62 21 2555 7956
Email: zacky.husein@ahp.id
URL: www.ahp.id

Zacky is the head of our technology, media and telecommunications (TMT) practice and has in-depth experience of regulatory issues concerning a full spectrum of TMT matters. Our TMT practice provides substantive input on transactions managed by other practice groups, such as mergers and acquisitions, banking and finance and projects, capital markets, and competition.

The TMT mandates that Zacky has been involved in include, among others, allocation of spectrum frequency for the telecommunication and broadcasting sector, financial innovation, digital technology and payment gateway, platform-based peer-to-peer lending, advising and drafting information and technology contracts, and cross-ownership compliance in the broadcasting, radio and print media.

Aside from advising and representing clients, Zacky has been active in providing substantive input during the discussion stages for various draft regulations being prepared by the Indonesian government – for example, regulations on network sharing and over-the-top services. Zacky also regularly speaks at industry and public seminars, in-house counsel forums, and corporate events related to TMT issues.

Muhammad Iqsan Sirie
Assegaf Hamzah & Partners
Capital Place, Level 36 & 37
Jalan Jenderal Gatot Subroto Kav. 18
Jakarta 12710
Indonesia
Tel: +62 21 2555 7805
Email: iqsan.sirie@ahp.id
URL: www.ahp.id

Iqsan has expertise in the technology, media and telecommunications (TMT) sector and has regularly advised on technology transactions and Indonesian laws and regulations issues related to new technologies and business models, such as over-the-top services, blockchain, cryptocurrency, cloud computing, big data, Internet of Things and artificial intelligence, for both domestic and international clients.

He also has a particular interest in data protection and privacy issues. He studied and wrote his Master’s thesis on this subject. During his Master’s at Leiden University, the Netherlands, he worked at a global pharmaceutical company where he handled the Benelux entities’ compliance with the EU’s General Data Protection Regulation.

Recently, he was seconded to one of Indonesia’s unicorns to assist their compliance with the Indonesian data protection and privacy laws and regulations.

**ASSEGAF HAMZAH & PARTNERS**

AHP’s Technology Media and Telecommunications (TMT) practice covers clients from all spectrums of the industry, from telecommunication operators, broadcasters, and service providers to digital players, content developers and investors. In the last several years, the TMT sector has expanded from its early focus on telecommunication infrastructure and procurement to cover applications and contents, as well as financial innovations, all of which are currently contributing to the most dynamic and exciting developments in the sector. Technology-led disruption in various sectors has also given rise to new models of business and new interactions between customers and service providers.

Our TMT practice works closely with our clients through this changing landscape. We also assist clients in ensuring compliance with new regulatory requirements.

Just as important as the breadth of our expertise, our clients appreciate our capacity to work seamlessly and collaboratively across practice areas, industries, and sectors in order to provide them with innovative tailor-made solutions.
Chapter 21

Ireland

Matheson

1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

Since 25 May 2018, the principal data protection legislation in Ireland has been Regulation (EU) 2016/679 (the “GDPR”), as supplemented by the Data Protection Acts 1988 to 2018 (collectively the “DPA”). The GDPR repealed Directive 95/46/EC and has led to increased (although not complete) harmonisation of data protection law across EU Member States. Irish law-specific nuances, as permitted or required under the GDPR, are set out in the DPA, which also implements Directive (EU) 2016/680 (the Law Enforcement Directive).

1.2 Is there any other general legislation that impacts data protection?

The following legislation also impacts data protection:

- The Freedom of Information Act 2014, which provides a legal right for persons to access information held by a body to which FOI legislation applies, to have official information relating to himself/herself amended where it is incomplete, incorrect or misleading, and to obtain reasons for decisions affecting him/her.
- The Protected Disclosures Act 2014 (the “Whistleblowers Act”), which provides a general suite of employment protections and legal immunities to whistle-blowers who raise a concern regarding wrongdoings in the workplace and may be at risk of penalisation as a result.
- The Criminal Justice (Mutual Assistance) Act 2008, Part 3, which enables Ireland to provide or seek various forms of mutual legal assistance to or from foreign law enforcement agencies.

Data protection in the electronics communications sector is also subject to S.I. No. 336/2011 the European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011 (the “2011 E-Privacy Regulations”). The 2011 E-Privacy Regulations implement the provisions of three Directives, namely Directive 2002/58/EC, Directive 2006/24/EC, and Directive 2009/136/EC. The 2011 E-Privacy Regulations apply to the processing of personal data in connection with the provision of publicly available electronic communications services in public communication networks in Ireland and, where relevant, in the EU. The 2011 E-Privacy Regulations also contain provisions relating to electronic marketing, which apply generally to all organisations engaging in such activities.

The European Commission has issued a proposal for a Regulation on Privacy and Electronic Communications to replace the existing legislative framework, which would have direct effect on EU Member States (the “Draft E-Privacy Regulation”). However, this remains in draft form as at the date of this guide.

The DPA applies in relation to (i) the processing of personal data for the purposes of safeguarding the security of, or the defence or international relations of, the State, and (ii) the processing of personal data under the Criminal Justice (Forensic Evidence and DNA Database System) Act 2014 or the Vehicle Registration Data (Automated Searching and Exchange) Act 2018 (to the extent the Data Protection Act 1988 is applied in those Acts). The DPA also applies to complaints and investigations brought prior to the introduction of the GDPR.

1.3 Is there any sector-specific legislation that impacts data protection?

The following sector-specific legislation impacts data protection:


1.4 What authority(ies) are responsible for data protection?

The Data Protection Commission (“DPC”) is the data protection supervisory authority responsible for ensuring that individuals’ data protection rights are protected and that the GDPR is enforced. The DPC is independent in the exercise of its functions and has powers to enforce the provisions of the GDPR and DPA – see section 16.

2 Definitions

2.1 Please provide the key definitions used in the relevant legislation:

- “Personal Data”
  Any information relating to an identified or identifiable natural
person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

- **“Processing”**
  Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

- **“Controller”**
  The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

- **“Processor”**
  A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

- **“Data Subject”**
  An identified or identifiable natural person who is the subject of relevant personal data.

- **“Sensitive Personal Data”**
  The term “Sensitive Personal Data” is replaced under the GDPR with the term “Special Categories of Personal Data”, being personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, and data concerning health or sex life and sexual orientation.

- **“Data Breach”**
  A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

*Other key definitions – please specify (e.g., “Pseudonymous Data”, “Direct Personal Data”, “Indirect Personal Data”)*

The following terms are set out in the GDPR:

- **“Genetic data”** means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question.

- **“Biometric data”** means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.

- **“Data concerning health”** means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.

There is no definition of “Pseudonymous Data”, “Direct Personal Data” or “Indirect Personal Data” under Irish law. However, the term “pseudonymisation” means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

### 3 Territorial Scope

#### 3.1 Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to those laws?

The GDPR applies to businesses that are established in Ireland (or any EU Member State), and that process personal data (either as a controller or processor, and regardless of whether or not the processing takes place in the EU) in the context of that establishment.

A business that is not established in any EU Member State, but is subject to the laws of an EU Member State by virtue of public international law, is also subject to the GDPR.

The GDPR applies to businesses located outside the EU if they (either as controller or processor) process the personal data of EU residents in the context of: (i) offering of goods or services (whether or not in return for payment) to such EU residents; or (ii) monitoring of the behaviour of such EU residents (to the extent that such behaviour takes place in the EU).

The European Data Protection Board (the “EDPB”) recently published Guidelines on the territorial scope of the GDPR (Guidelines 3/2018) which indicate that “establishment” extends to any real and effective activity (even a minimal one) exercised through stable arrangements (which, in some circumstances, could extend to the presence of a single employee or agent, if that employee or agent acts with a sufficient degree of stability).

### 4 Key Principles

#### 4.1 What are the key principles that apply to the processing of personal data?

- **Transparency**
  Personal data must be processed lawfully, fairly and in a transparent manner. Controllers must provide certain minimum information to data subjects regarding the collection and further processing of their personal data. Such information must be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language. The information must be provided at the time of collection of the personal data or, if the personal data is collected from a source other than the data subject, within a reasonable period after obtaining the personal data (and at the latest within one month).

- **Lawful basis for processing**
  Processing of personal data is lawful only if, and to the extent that, it is permitted under EU data protection law. The GDPR provides an exhaustive list of legal bases on which personal data may be processed, of which the following are the most relevant for businesses: (i) prior, freely given, specific, informed and unambiguous consent of the data subject; (ii) contractual necessity (i.e., the processing is necessary for the performance of a contract to which the data subject is a party, or for the purposes of pre-contractual measures taken at the data subject’s request); (iii) compliance with legal obligations (i.e., the controller has a legal obligation, under the laws of the EU or an EU Member State, to perform the relevant processing); or (iv) legitimate interests (i.e., the processing is necessary for the purposes of legitimate interests pursued by the controller, except where the controller’s interests are overridden by the interests, fundamental rights or freedoms of the affected data subjects).
The lawful bases for processing special categories of personal data are more narrowly drawn and such processing is only permitted under certain conditions, including the explicit consent of the data subject, where the processing is necessary in the context of employment law or for the protection of vital interests, and where the processing is necessary to assess the working capacity of an employee.

**Purpose limitation**
Personal data may only be collected for specified, explicit and legitimate purposes and must not be further processed in a manner that is incompatible with those purposes. If a controller wishes to use the relevant personal data in a manner that is incompatible with the purposes for which they were initially collected, it must: (i) inform the data subject of such new processing; and (ii) be able to rely on a lawful basis as described above.

**Data minimisation**
Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which those data are processed. A business should only process the personal data that it actually needs to process in order to achieve its processing purposes.

**Proportionality**
See ‘Data minimisation’ above.

**Accuracy**
Personal data must be accurate and, where necessary, kept up to date. A business must take every reasonable step to ensure that personal data that are inaccurate are either erased or rectified without delay.

**Retention**
Personal data must be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

**Other key principles – please specify**
- **Data security**
  See response to question 15.1.
- **Accountability**
  The controller is responsible for, and must be able to demonstrate on request, compliance with the data protection principles set out above. This requires controllers and processors to have robust and documented processes and procedures to ensure ongoing good governance and record-keeping.

## 5 Individual Rights

### 5.1 What are the key rights that individuals have in relation to the processing of their personal data?

**Right of access to data/copies of data**
A data subject has the right to obtain from a controller the following information in respect of the data subject’s personal data: (i) confirmation of whether, and where, the controller is processing the data subject’s personal data; (ii) information about the purposes of the processing; (iii) information about the categories of data being processed; (iv) information about the categories of recipients with whom the data may be shared; (v) information about the period for which the data will be stored (or the criteria used to determine that period); (vi) information about the existence of the rights to erasure, to rectification, to restriction of processing and to object to processing; (vii) information about the existence of the right to make a complaint to the relevant data protection authority; (viii) where the data were not collected from the data subject, information as to the source of the data; and (ix) information about the existence of, and an explanation of the logic involved in, any automated decision-making that has a significant effect on the data subject. The information may be provided by the controller to the data subject free of charge and within one month of receipt of the request (except in limited circumstances).

Additionally, the data subject may request a copy or a summary of the personal data being processed.

There are exceptions to data subject rights, including the right of access, which are set out in the DPA. The restrictions on data subjects’ access rights include where information is subject to legal privilege, were the information comprises an opinion of a third party given in confidence, or where personal data is processed for the purpose of estimating the amount of the liability of the controller on foot of a claim. In addition, the right of access to personal data must not adversely affect the rights of third parties.

**Right to rectification of errors**
Controllers must ensure that inaccurate or incomplete data are erased or rectified. Data subjects have the right to rectification of inaccurate personal data.

**Right to deletion/right to be forgotten**
Data subjects have the right to have their personal data erased (also known as the ‘right to be forgotten’) where: (i) the personal data is no longer necessary for the original purpose for which it was collected (and no new lawful basis for such processing exists); (ii) if the lawful basis for the processing is the data subject’s consent, the data subject withdraws that consent, and no other lawful basis for such processing exists; (iii) the data subject exercises his/her right to object to processing, and the controller has no overriding grounds for continuing the processing; (iv) the personal data has been unlawfully processed; (v) erasure is necessary for compliance with EU law or national data protection law to which the controller is subject; or (vi) if the data subject is a child, the personal data has been collected in relation to the offering of information society services.

**Right to object to processing**
Data subjects have the right to object, on grounds relating to their particular situation, to the processing of personal data where the basis for that processing is either public interest or legitimate interest of the controller. Where this right is exercised, the controller must cease such processing unless it is able to demonstrate compelling legitimate grounds for the processing which override the interests, rights and freedoms of the relevant data subject or requires the data in order to establish, exercise or defend legal rights.

**Right to restrict processing**
Data subjects have the right to restriction of processing of personal data (meaning the personal data may only be held by the controller, and may only be used for limited purposes) where: (i) the accuracy of the data is contested by the data subject (and only for as long as it takes to verify that accuracy); (ii) the processing is unlawful and the data subject requests restriction (as opposed to exercising the right to erasure); (iii) the controller no longer needs the data for its original purpose of processing, but the data is still required by the controller for the establishment, exercise or defence of legal rights; or (iv) verification of overriding grounds is pending, in the context of an erasure request.

**Right to data portability**
A data subject has a right to receive a copy of certain of his/her personal data in a commonly used machine-readable format, and to be able to transfer (or have transferred directly on his/her behalf) his/her personal data from one controller to another.
### Rights of data subjects

- **Right to withdraw consent**
  A data subject has the right to withdraw his/her consent at any time. The withdrawal of consent does not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject must be informed of the right to withdraw consent. It must be as easy to withdraw consent as to give it.

- **Right to object to marketing**
  Data subjects have the right to object to the processing of personal data for the purpose of direct marketing.

- **Right to complain to the relevant data protection authority(ies)**
  Data subjects have the right to lodge complaints concerning the processing of their personal data with the DPC if the data subject lives in Ireland or the alleged infringement occurred in Ireland.

**Other key rights – please specify**

- **Right to basic information**
  See question 4.1 (Transparency).

- **Breach notifications**
  Data subjects have the right to be informed of personal data breaches which are likely to result in high risk to their rights and freedoms.

- **Restrictions on data subject rights**
  None of the data subject rights set out in the GDPR is an absolute right, and each is subject to restrictions in certain circumstances, as specified in the GDPR and the DPA.

### Registration Formalities and Prior Approval

#### 6.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?

No, there is no requirement for a business to register or notify the DPC in respect of its processing activities. The previous requirement to register with the DPC was removed after the GDPR came into effect.

Data protection officers are required to be notified to the DPC (see question 7 below).

Whilst there is no obligation to notify the DPC, where a business has appointed a representative pursuant to Article 27 of the GDPR (i.e., where the business is not established in the EU but is caught by the GDPR by virtue of offering goods or services to EU data subjects or monitoring the behaviour of data subjects located in the EU), that representative must be designated in writing and its details must be easily accessible to the DPC in order to facilitate the establishment of contact for cooperation purposes.

#### 6.2 If such registration/notifications is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?

This is not applicable; please see question 6.1 above.

#### 6.3 On what basis are registrations/notifications made (e.g., per legal entity, per processing purpose, per data category, per system or database)?

This is not applicable; please see question 6.1 above.

#### 6.4 Who must register with/notify the data protection authority (e.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation)?

This is not applicable; please see question 6.1 above.

#### 6.5 What information must be included in the registration/notification (e.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes)?

This is not applicable; please see question 6.1 above.

#### 6.6 What are the sanctions for failure to register/notify where required?

This is not applicable; please see question 6.1 above.

#### 6.7 What is the fee per registration/notification (if applicable)?

This is not applicable; please see question 6.1 above.

#### 6.8 How frequently must registrations/notifications be renewed (if applicable)?

This is not applicable; please see question 6.1 above.

#### 6.9 Is any prior approval required from the data protection regulator?

This is not applicable; please see question 6.1 above.

#### 6.10 Can the registration/notification be completed online?

This is not applicable; please see question 6.1 above.

#### 6.11 Is there a publicly available list of completed registrations/notifications?

This is not applicable; please see question 6.1 above.

#### 6.12 How long does a typical registration/notification process take?

This is not applicable; please see question 6.1 above.
7 Appointment of a Data Protection Officer

7.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.

The appointment of a Data Protection Officer is mandatory for public authorities and for organisations whose core activities consist of (i) data processing operations which, by virtue of their nature, scope and purposes, require regular and systematic monitoring of data subjects on a large scale, or (ii) processing on a large scale of special categories of personal data or criminal convictions.

Where a business designates a Data Protection Officer voluntarily, the requirements of the GDPR in respect of data protection officers apply as though the appointment were mandatory.

In general, Irish law does not prescribe for the appointment of a Data Protection Officer beyond the requirements of the GDPR.

7.2 What are the sanctions for failing to appoint a Data Protection Officer where required?

Failure to appoint a Data Protection Officer where required (or a breach of other provisions of the GDPR relating to such appointment) may result in an administrative fine of up to €10 million or 2% of annual global turnover.

7.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect of his or her role as a Data Protection Officer?

Yes, the Data Protection Officer is an independent advisory function and must be free from disciplinary measures or other employment consequences for performing his/her tasks. He/she must also be free from conflicts of interest, must not receive any instructions in carrying out the function and must have access to the highest level of management in the organisation.

7.4 Can a business appoint a single Data Protection Officer to cover multiple entities?

Yes, group companies may jointly appoint a Data Protection Officer, provided that the Data Protection Officer is easily accessible by each member of the group. The role may also be outsourced to a third party.

7.5 Please describe any specific qualifications for the Data Protection Officer required by law.

The Data Protection Officer should be appointed on the basis of professional qualities and should have an expert knowledge of data protection law and practices. While this is not strictly defined, it is clear that the level of expertise required will depend on the circumstances. The DPC has published some guidance on appropriate qualifications for a Data Protection Officer on its website.

7.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?

A Data Protection Officer should be involved in all issues which relate to the protection of personal data. The GDPR outlines the minimum tasks required by the Data Protection Officer, which include: (i) informing the controller, processor and their relevant employees who process data of their obligations under the GDPR; (ii) monitoring compliance with the GDPR, national data protection legislation and internal policies in relation to the processing of personal data including internal audits; (iii) advising on data protection impact assessments and the training of staff; and (iv) co-operating with the data protection authority and acting as the authority’s primary contact point for issues related to data processing.

7.7 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?

Yes, the DPC must be notified and details of the DPO provided to it.

7.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?

Although it is not strictly required to name the Data Protection Officer (on an individual basis) in a public-facing privacy notice, the contact details of the Data Protection Officer must be notified to the data subject at the point the personal data is collected (so as a matter of practice, most organisations include the contact details, although not necessarily the name, of the Data Protection Officer in the privacy notice).

As a matter of good practice, the Article 29 Working Party (the “WP29”) (now the EDPB) recommended in its 2017 guidance on Data Protection Officers that both the DPC and employees within the organisation should be notified of the name and contact details of the Data Protection Officer.

8 Appointment of Processors

8.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?

Yes. The business that appoints a processor to process personal data on its behalf, is required to enter into an agreement with the processor which sets out the subject matter for processing, the duration of processing, the nature and purpose of processing, the types of personal data and categories of data subjects and the obligations and rights of the controller (i.e., the business), along with certain prescribed provisions set out in Article 28 of the GDPR.

It is essential that the processor appointed by the business complies with the GDPR.

8.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?

The processor must be appointed under a binding agreement in writing. The agreement should set out the subject matter, the duration, the nature and purpose of the processing, the types of personal data and categories of data subjects and the obligations and rights of the controller.

The contractual terms must stipulate that the processor: (i) only acts on the documented instructions of the controller; (ii) imposes
9 Marketing

9.1 Please describe any legislative restrictions on the sending of electronic direct marketing (e.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?).

The 2011 E-Privacy Regulations set out the rules in relation to electronic communications. The underlying principles of the GDPR must also be observed with regard to personal data processed for marketing purposes.

When using email or SMS to send messages to an individual for direct marketing purposes, the data subject’s prior opt-in consent must be obtained. Consent should meet the standard set out in the GDPR. However, a ‘soft opt-in’ applies where an entity is marketing its own same or similar products or services to an existing customer, subject to certain conditions. In limited circumstances, it may also be possible to market to business email addresses, unless the recipient objects.

Direct marketing communications must include the name, address and telephone number of the entity sending the marketing communications, and the recipient must be given the right to opt out of any subsequent marketing communication by a cost-free and easy method.

It is an offence under the 2011 E-Privacy Regulations to send communications without the requisite permissions.

The Draft E-Privacy Regulation will replace the 2011 E-Privacy Regulations once in force.

9.2 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.).

As per question 9.1 above, when using automatic dialling machines or fax to send messages to an individual, or making telephone calls to an individual or non-natural person’s mobile telephone, for direct marketing purposes, the data subject’s prior opt-in consent must be obtained.

The use of automatic dialling machines, fax, email or SMS for direct marketing to a non-natural person (i.e. a body corporate) is allowed as long as they have not recorded their objection in the National Directory Database (“NDD”), or they have not opted out of receipt of direct marketing.

The making of telephone calls for direct marketing to a subscriber or user is prohibited if the subscriber or user has recorded its objection in the NDD, or has opted out of receipt of direct marketing.

Where marketing materials are sent by post, data subjects have the right to object at any time to processing of personal data for direct marketing purposes. The right to object must be explicitly brought to the attention of the data subject and presented clearly and separately from any other information. Personal data must not be processed for marketing purposes where the data subject has objected to such processing.

9.3 Do the restrictions noted above apply to marketing sent from other jurisdictions?

The 2011 E-Privacy Regulations apply to the processing of personal data in connection with publicly available electronic communications services in public communications networks in Ireland and the European Community, so marketing sent from jurisdictions within the European Community are captured.

9.4 Is/are the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?

Yes, the DPC is, and traditionally has been, active in this area. By way of example, the DPC recently conducted an audit of a professional networking organisation in Ireland after becoming concerned with its use of non-member email addresses to engage in targeted advertising. The complaint was resolved amicably but demonstrates the DPC’s proactive approach in this area. A number of other investigations made under the 2011 E-Privacy Regulations concluded with successful District Court prosecutions by the DPC (against five entities in respect of a total of 30 offences).

9.5 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?

Although it is not unlawful in itself to purchase marketing lists, organisations may only contact the individuals on such marketing lists where those individuals have specifically consented (at the time their contact details were collected) to receipt of marketing communications and to the sharing of their personal data for those purposes (subject to the ‘soft opt-in’ described under question 9.1 above). In practical terms, the circumstances in which an organisation will be entitled, under the GDPR and the 2011 E-Privacy Regulations, to make use of a marketing list purchased by it, will be limited.

In respect of telephone calls, the NDD (see question 9.2 above) contains details of subscribers who have expressed a preference not to receive marketing calls to landlines, or alternatively have positively indicated consent to receipt of marketing to mobile phones. Companies using bought-in lists to engage in direct marketing calls by telephone should therefore consult the NDD (and any internal lists of numbers which should not be contacted) in advance of the use of any purchased lists.

9.6 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?

Under the 2011 E-Privacy Regulations, it is an offence to send electronic communications in breach of applicable restrictions. The penalties for such offences are:

- on summary conviction, a fine of €5,000; or
- on indictment, a fine of €250,000 where the offender is a body corporate or, in the case of a natural person, a fine of €50,000.
A court order for the destruction or forfeiture of any data connected with the breach may also be issued. Each breaching communication constitutes an independent offence under the 2011 E-Privacy Regulations.

There is some overlap between the 2011 E-Privacy Regulations and the GDPR. Where a breach of the GDPR occurs in relation to the sending of marketing communications (for example, where the appropriate level of consent has not been sought), the business may be subject to an administrative fine under the GDPR.

10 Cookies

10.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).

Under the 2011 E-Privacy Regulations, consent is required for cookies which are not strictly necessary for a transaction that the data subject has explicitly requested. The user must be given clear information in relation to what he/she is being asked to consent to in terms of cookie usage, and the means of consenting should be as user-friendly as possible.

The Draft E-Privacy Regulation, when in force, will replace the 2011 E-Privacy Regulations.

The forthcoming decision of the Court of Justice of the European Union in the Planet49 case will provide further guidance on cookie transparency and consent.

10.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?

Under the 2011 E-Privacy Regulations, consent is required for cookies which are not strictly necessary for a transaction that the data subject has explicitly requested. The user must be given clear information in relation to what he/she is being asked to consent to in terms of cookie usage, and the means of consenting should be as user-friendly as possible. Consent is not required where cookies are strictly necessary to provide the service being sought (for example, in order to provide a functioning website).

10.3 To date, has/have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?

The DPC has been active in this field, but has not yet taken any public enforcement actions. The DPC has also published guidance on its website to assist companies and organisations which use cookies.

10.4 What are the maximum penalties for breaches of applicable cookie restrictions?

The penalties for breaches of applicable cookie restrictions under the 2011 E-Privacy Regulations are as follows:

- on summary conviction, a fine of €5,000; or
- on indictment, a fine of €250,000 where the offender is a body corporate or, in the case of a natural person, a fine of €50,000.

A court order for the destruction or forfeiture of any data connected with the breach may also be issued.

As discussed above, there is some overlap between the 2011 E-Privacy Regulations and the GDPR. Where a breach of the GDPR occurs in relation to the placement of cookies (for example, where the appropriate level of consent has not been sought), the business may be subject to an administrative fine under the GDPR.

11 Restrictions on International Data Transfers

11.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.

Personal data may not be transferred from Ireland outside the European Economic Area (“EEA”) unless one of the following applies:

(a) the personal data is transferred to a jurisdiction in respect of which a finding of adequacy has been made by the European Commission (see also question 11.2 in relation to the EU-US Privacy Shield);

(b) the transfer is made on the basis of the European Commission’s pre-approved standard contractual clauses between the controller and the person/organisation to whom it intends to transfer the information abroad, which ensure an appropriate level of protection for the personal data (which do not require the approval of the DPC);

(c) the transfer is made on the basis of intra-group binding corporate rules (“BCRs’), which have been approved by the DPC or another data protection supervisory authority in another EEA jurisdiction;

(d) the transfer is made on the basis of an approved code of conduct pursuant to Article 40 of the GDPR, together with binding and enforceable commitments of the organisation in the third country to apply the appropriate safeguards, including as regards data subject rights;

(e) the transfer is made on the basis of an approved certification mechanism pursuant to Article 42 of the GDPR, together with binding and enforceable commitments of the organisation in the third country to apply the appropriate safeguards, including as regards data subject rights;

(f) the transfer is made pursuant to a legally binding and enforceable instrument between public authorities or bodies; or

(g) one of the derogations specified in the GDPR applies to the relevant transfer (in limited circumstances).

Following the withdrawal of the United Kingdom from the European Union, the United Kingdom will become a ‘third country’ for the purposes of data protection law and, unless a finding of adequacy is made by the European Commission, one of the safeguarding mechanisms described above must be implemented in respect of transfers of personal data from the EEA to the United Kingdom.

11.2 Please describe the mechanisms businesses typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).

See question 11.1.

Transfers of personal data to the United States of America ("US") are permitted where the US entity receiving the personal data has signed up to the EU-US Privacy Shield framework, which was designed by the US Department of Commerce and the European Commission to provide businesses in the EU and the US with a mechanism to facilitate the transfer of personal data from the EU to the US.
11.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.

Where transfers of personal data to other jurisdictions are made pursuant to standard contractual clauses approved by the European Commission, the DPC does not need to be notified of the transfer. If personal data is transferred outside the EEA under contracts which vary the provisions of the standard contractual clauses, the transfer must be notified to and approved by the DPC. There is no requirement to deposit the contracts with the DPC once the process is complete. The DPC will only consider authorising contracts that are general in nature (e.g. standard contractual clauses that can be relied upon by a number of different controllers within a sector or category, rather than specific contracts). The length of time this process takes varies depending on the nature of the modifications to the standard contractual clauses.

The DPC or another data protection authority must approve BCRs which are intended to be used to transfer personal data outside the EEA within a corporate group. This requires engagement with the DPC or another EEA data protection authority by the organisation involved. Use of BCRs has not, traditionally, been significant, given that the DPC must review the BCRs in advance and it is considered to be a lengthy process. However, the Annual Report of the DPC covering the period 25 May 2018 to 31 December 2018 indicates that the DPC has continued to act or has commenced acting as lead reviewer on 11 BCR applications.

12 Whistle-blower Hotlines

12.1 What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?

The Whistleblowers Act covers both the public and private sectors and has been recognised as providing significant levels of protection to whistle-blowers across the EU. Employers must ensure that existing internal whistle-blower policies, and more generally, how they address such matters, are aligned with the requirements of the Whistleblowers Act. In accordance with international best practice, the safeguards in the Act are extended to a wide range of ‘workers’ and the concept of ‘worker’ is broadly defined to include employees, independent contractors, trainees, agency staff, and certain individuals on work experience.

The Whistleblowers Act provides an exhaustive list of ‘relevant wrongdoings’ (i.e., the scope of issues that may be reported) as follows:

- that an offence has been, is being or is likely to be committed;
- that a person has failed, is failing or is likely to fail to comply with any legal obligation, other than one arising under the worker’s contract of employment or other contract whereby the worker undertakes to do or perform personally any work or services;
- that a miscarriage of justice has occurred, is occurring or is likely to occur;
- that the health or safety of any individual has been, is being or is likely to be endangered;
- that the environment has been, is being or is likely to be damaged;
- that an unlawful or otherwise improper use of funds or resources of a public body, or of other public money, has occurred, is occurring or is likely to occur;
- that an act or omission by or on behalf of a public body is oppressive, discriminatory or grossly negligent or constitutes gross mismanagement; or
- that information tending to show any matter falling within any of the preceding paragraphs has been, is being or is likely to be concealed or destroyed.

The Whistleblowers Act imposes an obligation on the part of the recipient of a protected disclosure not to disclose any information that may identify the person who made the protected disclosure, unless:

- the recipient can show that he/she took all reasonable steps to avoid disclosing any such information;
- the recipient reasonably believes that the person making the disclosure does not object to the disclosure of any such information;
- the recipient reasonably believes that disclosing such information is necessary for the effective investigation of the relevant wrongdoing; the prevention of serious risk to the security of the State, public health, public safety or the environment; or the prevention of crime or prosecution of a criminal offence; or
- the disclosure is otherwise necessary in the public interest or is required by law.

The Whistleblowers Act provides a number of avenues to workers for making a protected disclosure.

13 CCTV

13.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?

The use of CCTV does not require prior approval from the DPC. However, controllers or processors using CCTV must comply with their general obligations under the GDPR in the use of CCTV cameras and footage (including that such processing must have a lawful basis). Appropriate notification must be given to individuals who may be recorded via CCTV cameras (e.g. a visible sign or in an applicable policy).

The DPC, in its Annual Report covering the period from 25 May 2018 to 31 December 2018, indicated that its Special Investigations Unit has opened 31 own-volition inquiries under the DPA into the surveillance of citizens by the state sector for law enforcement purposes through the use of technologies including CCTV.

13.2 Are there limits on the purposes for which CCTV data may be used?

See question 13.1 above in relation to compliance with data protection obligations.
14 Employee Monitoring

14.1 What types of employee monitoring are permitted (if any), and in what circumstances?

There are no particular restrictions around the types of monitoring which may be used in respect of employees (e.g. monitoring of electronic communications or surveillance by CCTV). However, given that the act of monitoring involves the collection of personal data, the principles outlined in question 4.1 above must be adhered to (particularly the principles around transparency and proportionality).

Any employee monitoring by employers must strike an appropriate balance between the legitimate aims of the employer and the privacy rights of the employees in question. For example, consistent monitoring of employees by CCTV would be difficult to justify, except where there is a specific security need. Employers should be certain that they will be able to meet their obligations to provide data subjects, on request, with copies of their captured images.

Employees have a legitimate expectation of privacy in relation to certain communications made from the workplace, and any monitoring should be clearly set out in an applicable policy.

14.2 Is consent or notice required? Describe how employers typically obtain consent or provide notice.

Employees must be notified of the existence of monitoring and the purposes for which the data are processed (which is usually achieved through an appropriate privacy notice). While consent is not required, the employer must have a lawful basis for the monitoring, which must be proportionate. Covert monitoring is almost never justified, with the possible exception of criminal investigations.

14.3 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?

The extent to which a works council/trade union/employee representative needs to be notified of such surveillance will depend on: (i) the scope of the agreement with the relevant body; (ii) whether this topic has already been covered in the contract of employment; and (iii) the likelihood that the employer will need to rely on the monitoring in the future (in order to provide evidence in defending a claim from an employee, for example).

15 Data Security and Data Breach

15.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?

Yes, there is a general obligation under the GDPR to ensure the security of processing of personal data.

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, organisations must implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk (in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed).

Depending on the risk, such measures may include (as appropriate): (i) pseudonymisation and encryption of personal data; (ii) the ability to ensure the ongoing confidentiality, integrity and resilience of processing systems and services; (iii) an ability to restore the availability and access to personal data in a timely manner following a technical or physical incident; and (iv) a process for regularly testing, assessing and evaluating the technical and organisational measures for ensuring the security of processing.

15.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

Yes, a controller must report a personal data breach without undue delay (and in any case within 72 hours of first becoming aware of the breach) to the DPC, unless the breach is unlikely to result in a risk to the rights and freedoms of the data subject(s). A processor must notify any data breach to the controller without undue delay.

The notification by the controller to the DPC must describe the nature of the personal data breach including the categories and number of data subjects concerned, communicate the name and contact details of the Data Protection Officer or relevant point of contact, describe the likely consequences of the breach and describe the measures proposed to be taken by the controller to address and/or mitigate the breach.

15.3 Is there a legal requirement to report data breaches to affected data subjects? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

Controllers have a legal requirement to communicate a breach to affected data subjects without undue delay, where the breach is likely to result in a high risk to the rights and freedoms of the data subjects.

The communication must describe in clear and plain language the nature of the personal data breach, include the name and contact details of the Data Protection Officer (or point of contact), describe the likely consequences of the breach, and describe any measures proposed to be taken by the controller to address and/or mitigate the breach.

The controller may be exempt from notifying the data subject if the risk of harm is remote (e.g., because the affected data is encrypted), the controller has taken measures to minimise the risk of harm (e.g., suspending affected accounts), or the notification requires a disproportionate effort (e.g., a public notice of the breach).

15.4 What are the maximum penalties for data security breaches?

The maximum penalty is the higher of €10 million or 2% of global annual turnover.
16 Enforcement and Sanctions

16.1 Describe the enforcement powers of the data protection authority(ies).

<table>
<thead>
<tr>
<th>Investigatory Power</th>
<th>Civil/Administrative Sanction</th>
<th>Criminal Sanction</th>
</tr>
</thead>
<tbody>
<tr>
<td>Investigation Powers</td>
<td>The DPC (and its authorised officers) has broad powers under the DPA to enter business premises, including the right to: (i) access, search and inspect any premises where processing of personal data takes place and the documents, records, statements or other information found there; (ii) require any employees to produce any documents, records, statements or other information relating to the processing of personal data (or direct the authorised officers to where they might be located); (iii) secure for later inspection any documents, records, equipment or place in which records may be held; (iv) inspect, take extracts, make copies or remove and retain such documents and records as considered necessary; and (v) require any person referred to in (iii) above to give the authorised officer any information relating to the processing of personal data that the officer may reasonably require for performing his/her functions. The DPC may also conduct investigations in the form of data protection audits, issue information and enforcement notices (and require the controller/processor to take certain steps specified in the enforcement notice), require the controller/processor to provide a report on any matter, and, where it considers that there is an urgent need to act in order to protect the rights and freedoms of data subjects, apply to the High Court for an order suspending, restricting or prohibiting processing.</td>
<td></td>
</tr>
<tr>
<td>Corrective Powers</td>
<td>The data protection authority has a wide range of powers, including to issue warnings or reprimands for non-compliance, to order the controller to disclose a personal data breach to the data subject, to impose a permanent or temporary ban on processing, to withdraw a certification, and to impose an administrative fine (as below).</td>
<td></td>
</tr>
<tr>
<td>Authorisation and Advisory Powers</td>
<td>The data protection authority has a wide range of powers to advise the controller, accredit certification bodies and to authorise certificates, contractual clauses, administrative arrangements and binding corporate rules, as outlined in the GDPR.</td>
<td></td>
</tr>
<tr>
<td>Imposition of administrative fines for infringements of specified GDPR provisions</td>
<td>The GDPR provides for administrative fines which can be up to €20 million or up to 4% of the business’ worldwide annual turnover of the preceding financial year.</td>
<td></td>
</tr>
<tr>
<td>Non-compliance with a data protection authority</td>
<td>The GDPR provides for administrative fines which can be up to €20 million or up to 4% of the business’ worldwide annual turnover of the preceding financial year, whichever is higher.</td>
<td></td>
</tr>
</tbody>
</table>

16.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?

The GDPR and the DPA entitle the DPC to impose a temporary or definitive limitation, including a ban on processing.

16.3 Describe the data protection authority’s approach to exercising those powers, with examples of recent cases.

The DPC exercises all of the powers referred to in question 16.1 on a regular basis. The DPC has conducted investigations on, obtained information from, and conducted audits and inspections of, many organisations. The DPC carried out 20 audits and inspections on major holders of personal data in the public and private sectors between 1 January and 24 May 2018. It also indicated in its Annual Report, covering the period from 25 May 2018 to 31 December 2018, that its Special Investigations Unit has opened 31 own-volition inquiries under the DPA into the surveillance of citizens by the state sector for law enforcement purposes through the use of technologies including CCTV.

Since 25 May 2018, the DPC has opened 15 statutory enquiries in relation to multinational technology companies’ compliance, and 35 in relation to Irish companies’ compliance, with the GDPR.

In 2018, the DPC commenced a project to develop a new five-year regulatory strategy, which will include extensive external consultation during the course of 2019.

16.4 Does the data protection authority ever exercise its powers against businesses established in other jurisdictions? If so, how is this enforced?

The DPC has the ability under the GDPR to enforce against businesses established in other jurisdictions where such businesses fall within the scope of the GDPR (i.e., where they are carrying out processing activities related to the offering of goods or services to, or monitoring the behaviour of, data subjects in the EU). The DPC is able to enforce its powers through the business’s representative, which is required to be appointed pursuant to Article 27 of the GDPR.
17.1 How do businesses typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?

Where personal data are sought for use in civil proceedings in a foreign country, Irish companies may be compelled, under a subpoena from an Irish court, to provide them. This happens frequently between EU countries, but it is also possible for a request from outside the EU to succeed.

In relation to requests from foreign law enforcement agencies, there is a legal framework in place that allows for the law enforcement agencies of foreign signatories of certain Hague Conventions to seek the disclosure of data held by Irish companies by the Irish police, who then issue a warrant for them. Where the request is made by the law enforcement agencies of countries who are not signatories to the Hague Conventions, the request will be determined by the Department of Justice and Equality on a case-by-case basis. Generally, where proper undertakings are given by the agency making the request, it will be granted, and Irish companies will be compelled to disclose the personal data.

17.2 What guidance has/have the data protection authority(ies) issued?

The DPC has not, as yet, issued official guidance in relation to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies.

18.1 What enforcement trends have emerged during the previous 12 months? Describe any relevant case law.

There have been over 2,860 complaints submitted to the DPC since 25 May 2018 (of which the GDPR applies to approximately 2,000). Complaints in relation to data access requests account for the highest volume of complaints, making up 977 of the complaints filed. Additionally, cross-border issues, rights of erasure and deletion are emerging as a significant category of complaints.

The DPC has issued 18 formal decisions since 25 May 2018. Of these, 13 upheld the complaint and five rejected the complaint. A number of investigations made under the 2011 E-Privacy Regulations concluded with successful District Court prosecutions by the DPC against five entities in respect of a total of 30 offences.

The DPC is engaged in ongoing litigation with Facebook in the Supreme Court on the validity of standard contractual clauses.

Brexit is a key focus area at present. The DPC issued guidance in December 2018 clarifying that in the event of a ‘hard’ Brexit, where the United Kingdom leaves the EU without the Withdrawal Agreement being implemented, the United Kingdom will become, with immediate effect, a ‘third country’ for the purposes of the GDPR.

Without a finding of adequacy by the European Commission (or similar arrangement to permit the lawful transfer of data to the United Kingdom without a finding of adequacy), organisations transferring personal data from the EEA to the United Kingdom will accordingly be required to put in place a safeguarding mechanism. See question 11.1. The DPC has commented that approximately 70% of small and medium-sized enterprises in Ireland have never traded outside the EU and are accordingly unfamiliar with the international transfer mechanism. The DPC has produced templates to assist such organisations in achieving compliance with the requirements by the date on which the United Kingdom leaves the EU, if required. If the Withdrawal Agreement does come into effect, the status quo will remain while negotiations take place.

Data breaches are another focus area. Between 25 May 2018 and 31 December 2018, the DPC received 3,687 data breach notifications and handled 48 data breach complaints, including a number of complaints against the Central Statistics Office in relation to the disclosure of P45 details.

The DPC has expressed interest in CCTV recording, dashcams and bodycams (having published recent guidance on these topics) as well as ‘connected vehicles’, and it is anticipated that the DPC will be actively looking at organisations operating in these spaces. It is also running consultations at present on children’s rights and the DPC’s regulatory strategy.

Overall, there is an enhanced awareness of data subject rights and a rise in the uptake and exercise of those rights.
Anne-Marie Bohan has over 20 years’ experience in technology-related legal matters, and is Head of Matheson’s Technology and Innovation Group and a member of our Asset Management and Investment Funds Group. Anne-Marie brings together significant practical experience in advising on technology and privacy legal issues, with industry knowledge and an understanding of applicable regulatory rules and regulatory requirements. She advises on all aspects of technology and e-commerce law, as well as outsourcings and contracted services, with particular focus on the requirements of financial institutions and financial services providers in these areas.

Anne-Marie has extensive experience in drafting and negotiating contracts for the development, sale, purchase and licensing of hardware, software and IT systems for both suppliers and users of IT within the financial services industry and across a broad range of other industries. She has also acted in some of the highest-value and most complex outsourcing contracts for IT and telecommunications systems and services, including advising on a number of the most significant financial services outsourcings in Ireland.

Matheson has the longest established technology law practice in Ireland, set up more than 20 years ago. Over that period, we have advised the tech sector and blue-chip technology companies in Ireland, including multi-nationals in relation to their technology-related work, consistently and with a specialised focus, and have been involved at the cutting edge of technology-related legal developments. The Technology and Innovation Group’s expertise spans the full spectrum of technology infrastructure, products and services.

Our specialised team of technology-focused lawyers have a breadth and depth of transactional and advisory experience that is unrivalled. We act for some of the largest multinational ICT companies with operations in Ireland, as well as some of the main corporate and public sector users of information technology in the country, and have advised on many of the largest and most complex IT, computer and systems integration, outsourcing, cloud computing and managed services contracts in Ireland. We advise a large number of software, hardware, technology and internet multinational organisations, and are involved in both national and international technology legal work, as well as in some of the largest technology-based transactions and initiatives in Ireland.
Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

The principal data protection legislation is the Data Protection Act 2018, which is supplemented by the GDPR and LED Implementing Regulations 2018 (the “Regulations”) as well as the Data Protection (Application of GDPR) Order 2018 and the Data Protection (Application Of LED) Order 2018 (the “Orders”).

1.2 Is there any other general legislation that impacts data protection?

The Regulations anticipate that the Information Commissioner (the “ICO”) will issue a data sharing Code, a direct marketing Code and any other Codes required to be issued by the Council of Ministers. These have generally not been issued at the time of writing, although a number of the Codes of Practice previously issued by the ICO remain of relevance. The ICO has also issued a number of “Closer Look” guides to support compliance with the Regulations and the Orders.

1.3 Is there any sector-specific legislation that impacts data protection?

The 2016 Code of Practice on Access to Government Information imposes additional data compliance obligations on government departments and public sector workers.

1.4 What authority(ies) are responsible for data protection?

The ICO is the independent supervisory body for data protection. The ICO is also the supervisory body for the current Unsolicited Communications Regulations from 2005 (“UCR”), holds certain responsibilities in respect of the Isle of Man Government’s Code of Practice on Access to Government Information and holds an adjudication role in respect of the Freedom of Information Act 2015.

Definitions

2.1 Please provide the key definitions used in the relevant legislation:

- **“Personal Data”**
  
  The Regulations currently define personal data as meaning “any information relating to an identified or identifiable living individual”. “Identifiable living individual” is further defined to mean “a living individual who can be identified, directly or indirectly, in particular by reference to: (a) an identifier such as a name, an identification number, location data or an online identifier; or (b) one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual”.

- **“Processing”**
  
  “Processing” means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

- **“Controller”**
  
  “Controller” means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. This definition is, however, qualified by the Regulations so that where data is processed only: (a) for purposes for which it is required by an enactment to be processed; and (b) by means which an enactment required to be used for such processing, the controller is the person on whom the obligation to process the data is imposed by the enactment or any one of the enactments (if there are more than one). The definition is also subject to the provisions on the application of the Regulations to the Crown and to Tynwald (the Isle of Man Parliament).

- **“Processor”**
  
  “Processor” means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

- **“Data Subject”**
  
  “Data Subject” means the identified or identifiable living individual to whom personal data relates.

- **“Sensitive Personal Data”**
  
  “Sensitive Personal Data” are personal data revealing racial or ethnic origin, political opinions, religious or philosophical...
beliefs, trade-union membership, data concerning health or sex life and sexual orientation, genetic data or biometric data. This is now referred to as “Special Category Data” for the purposes of the Regulations and the Orders.

- **“Data Breach”**
  “Data Breach” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

- **Other key definitions – please specify (e.g., “Pseudonymous Data”, “Direct Personal Data”, “Indirect Personal Data”)**
  “Biometric data” means personal data resulting from specific technical processing, relating to the physical, physiological or behavioural characteristics of an individual, which allow or confirm the unique identification of that individual, such as facial images or dactyloscopic data.

“Data concerning health” means personal data relating to the physical or mental health of an individual, including the provision of healthcare services, which reveal information about his or her health status.

“Genetic data” means personal data relating to the inherited or acquired genetic characteristics of an individual which give unique information about the physiology or the health of that individual and which result, in particular, from an analysis of a biological sample from the individual in question.

### 3 Territorial Scope

#### 3.1 Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to those laws?

The Regulations apply to the following:

- A data controller established in the Island where the personal data is processed in the context of the activities of that establishment.

- A data processor processing personal data where the data processor is established in the Island and the personal data is processed in the context of the activities of that establishment.

- A data controller or data processor processing personal data where the data controller or data processor is not established in the Island but uses equipment in the Island for processing the personal data other than for the purposes of transit through the Island.

- A data controller established outside the Island where the personal data being processed relate to an individual who is in the Island when the processing takes place and the purpose of the processing is to offer goods or services to individuals in the Island, whether or not for payment or to monitor individuals’ behaviour in the Island.

- A data processor processing personal data for a data controller outside the Island or a data processor outside the Island where the personal data being processed relate to an individual who is in the Island when the processing takes place and the purpose of the processing is to offer goods or services to individuals in the Island, whether or not for payment or to monitor individuals’ behaviour in the Island.

### 4 Key Principles

#### 4.1 What are the key principles that apply to the processing of personal data?

- **Transparency**
  Personal data must be processed lawfully, fairly and in a transparent manner. Controllers must provide certain minimum information to data subjects regarding the collection and further processing of their personal data. Such information must be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

- **Lawful basis for processing**
  Processing of personal data is lawful only if, and to the extent that, it is permitted under Isle of Man data protection law. The law provides an exhaustive list of legal bases on which personal data may be processed, of which the following are the most relevant for businesses: (i) prior, freely given, specific, informed and unambiguous consent of the data subject; (ii) contractual necessity (i.e., the processing is necessary for the performance of a contract to which the data subject is a party, or for the purposes of pre-contractual measures taken at the data subject’s request); (iii) compliance with legal obligations (i.e., the controller has a legal obligation to perform the relevant processing); or (iv) legitimate interests (i.e., the processing is necessary for the purposes of legitimate interests pursued by the controller, except where the controller’s interests are overridden by the interests, fundamental rights or freedoms of the affected data subjects).

Please note that businesses require stronger grounds to process special category personal data. The processing of special category personal data is only permitted under certain conditions, of which the most relevant for businesses are: (i) prior, freely given, specific, informed and unambiguous consent of the data subject; (ii) the processing is necessary in the context of employment law; or (iii) the processing is necessary for the establishment, exercise or defence of legal claims.

- **Purpose limitation**
  Personal data may only be collected for specified, explicit and legitimate purposes and must not be further processed in a manner that is incompatible with those purposes. If a controller wishes to use the relevant personal data in a manner that is incompatible with the purposes for which they were initially collected, it must: (i) inform the data subject of such new processing; and (ii) be able to rely on a lawful basis as set out above.

- **Data minimisation**
  Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which those data are processed. A business should only process the personal data that it actually needs to process in order to achieve its processing purposes.

- **Proportionality**
  Personal data must be accurate and, where necessary, kept up to date. A business must take every reasonable step to ensure that personal data that are inaccurate are either erased or rectified without delay.

- **Retention**
  Personal data must be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

- **Other key principles – please specify**
  
  - **Data security**
    Personal data must be processed in a manner that ensures appropriate security of those data, including protection against...
unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

**Accountability**

The controller is responsible for, and must be able to demonstrate, compliance with the data protection principles set out above.

### 5 Individual Rights

#### 5.1 What are the key rights that individuals have in relation to the processing of their personal data?

- **Right of access to data/copies of data**
  
  A data subject has the right to obtain from a controller the following information in respect of the data subject’s personal data: (i) confirmation of whether, and where, the controller is processing the data subject’s personal data; (ii) information about the purposes of the processing; (iii) information about the categories of data being processed; (iv) information about the categories of recipients with whom the data may be shared; (v) information about the period for which the data will be stored (or the criteria used to be determine that period); (vi) information about the existence of the rights to erasure, to rectification, to restriction of processing and to object to processing; (vii) information about the existence of the right to complain to the relevant data protection authority; (viii) where the data were not collected from the data subject, information as to the source of the data; and (ix) information about the existence of, and an explanation of the logic involved in, any automated processing that has a significant effect on the data subject. Additionally, the data subject may request a copy of the personal data being processed.

- **Right to rectification of errors**
  
  Controllers must ensure that inaccurate or incomplete data are erased or rectified. Data subjects have the right to rectification of inaccurate personal data.

- **Right to deletion/right to be forgotten**
  
  Data subjects have the right to erasure of their personal data (the “right to be forgotten“) if: (i) the data are no longer needed for their original purpose (and no new lawful purpose exists); (ii) the lawful basis for the processing is the data subject’s consent, the data subject withdraws that consent, and no other lawful ground exists; (iii) the data subject exercises the right to object, and the controller has no overriding grounds for continuing the processing; (iv) the data have been processed unlawfully; or (v) erasure is necessary for compliance with data protection law.

- **Right to object to processing**
  
  Data subjects have the right to object, on grounds relating to their particular situation, to the processing of personal data where the basis for that processing is either public interest or legitimate interest of the controller. The controller must cease such processing unless it demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the relevant data subject or requires the data in order to establish, exercise or defend legal rights.

- **Right to restrict processing**
  
  Data subjects have the right to restrict the processing of personal data, which means that the data may only be held by the controller, and may only be used for limited purposes if: (i) the accuracy of the data is contested (and only for as long as it takes to verify that accuracy); (ii) the processing is unlawful and the data subject requests restriction (as opposed to exercising the right to erasure); (iii) the controller no longer needs the data for their original purpose, but the data are still required by the controller to establish, exercise or defend legal rights; or (iv) verification of overriding grounds is pending, in the context of an erasure request.

- **Right to data portability**
  
  Data subjects have a right to receive a copy of their personal data in a commonly used machine-readable format, and to transfer their personal data from one controller to another or have the data transmitted directly between controllers.

- **Right to withdraw consent**
  
  A data subject has the right to withdraw their consent at any time. The withdrawal of consent does not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject must be informed of the right to withdraw consent. It must be as easy to withdraw consent as to give it.

- **Right to object to marketing**
  
  Data subjects have the right to object to the processing of personal data for the purpose of direct marketing, including profiling.

- **Right to complain to the relevant data protection authority(ies)**
  
  Data subjects have the right to lodge complaints concerning the processing of their personal data with the ICO, if the data subjects live in the Isle of Man or the alleged infringement occurred in the Isle of Man.

- **Other key rights – please specify**
  
  Data subjects have the right to be provided with information on the identity of the controller, the reasons for processing their personal data and other relevant information necessary to ensure the fair and transparent processing of personal data.

### 6 Registration Formalities and Prior Approval

#### 6.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?

Personal data must not be processed unless an entry in respect of the data controller is included in the register maintained by the ICO. The registration requirement also extends to data processors.

#### 6.2 If such registration/notification is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?

Registration is limited to some basic information in relation to the controller or processor, including the nature of its business and the details of the Data Protection Officer or other appropriate contact.

#### 6.3 On what basis are registrations/notifications made (e.g., per legal entity, per processing purpose, per data category, per system or database)?

Registration is required on a “per data controller” or a “per data processor” basis.
The Regulations require every controller and processor to which the Data Protection (Application of GDPR) Order 2018 (the “applied GDPR”) applies, to register subject to certain exemptions which are set out in Schedule Seven to the Regulations. Question 4.1 above sets out the scope of the Regulations in terms of the entities to which they apply.

Registration is limited to some basic information in relation to the controller or processor, including the nature of its business and the details of the Data Protection Officer or other appropriate contact.

Controllers and processors commit an offence if they process data without a registration when there is no applicable exemption, and when they fail to notify the ICO of changes to their registration information. These offences carry fines of up to £10,000 and directors may also be personally liable for offences.

Fees are prescribed by Treasury in the Data Protection (Fees) Regulations 2018. The fees are currently set at £70 although the ICO notes that the Council of Ministers may decide to amend that in the future. Exemptions from fees are available for relevant bodies where processing is limited to certain activities.

Registration must be renewed annually.

Prior approval in advance of registration is not required.

The registration can be completed online via the ICO’s website.

There is a publicly available list of completed registrations/notifications which is available on the ICO’s website. Separate lists are available of those who remain registered under the Data Protection Act 2002 and those who are registered under the Regulations.
including: (i) informing the controller, processor and their relevant employees who process data of their obligations under the law; (ii) monitoring compliance with data protection legislation and internal policies in relation to the processing of personal data including internal audits; (iii) advising on data protection impact assessments and the training of staff; and (iv) co-operating with the data protection authority and acting as the authority’s primary contact point for issues related to data processing.

7.7 Must the appointment of a Data Protection Officer be registered/ notified to the relevant data protection authority(ies)?

Yes, the controller or processor must notify the data protection authority of the contact details of the designated Data Protection Officer.

7.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?

The Data Protection Officer does not necessarily need to be named in the public-facing privacy notice. However, the contact details of the Data Protection Officer must be notified to the data subject when personal data relating to that data subject are collected.

8 Appointment of Processors

8.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?

Yes. The business that appoints a processor to process personal data on its behalf is required to enter into an agreement with the processor which sets out the subject matter for processing, the duration of processing, the nature and purpose of processing and the obligations and rights of the controller (i.e., the business).

It is essential that the processor appointed by the business complies with data protection requirements.

8.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?

The processor must be appointed under a binding agreement in writing. The contractual terms must stipulate that the processor: (i) only acts on the documented instructions of the controller; (ii) imposes confidentiality obligations on all employees; (iii) ensures the security of personal data that it processes; (iv) abides by the rules regarding the appointment of sub-processors; (v) implements measures to assist the controller with guaranteeing the rights of data subjects; (vi) assists the controller in obtaining approval from the Data Protection Officer; (vii) either returns or destroys the personal data at the end of the relationship; and (viii) provides the controller with all the information necessary to demonstrate compliance with the data protection requirements.

9 Marketing

9.1 Please describe any legislative restrictions on the sending of marketing communications (e.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?).

The following provisions apply:

- Direct marketing activities must generally comply with the Regulations, and the applied GDPR and direct marketing communicated by electronic messages (including email, SMS and picture messaging) must comply with the UCR.
- Persons marketing by way of electronic mail (SMS, email or picture messaging) must obtain consent of the individual prior to transmission, or instigation of transmission, unless the conditions of a “soft opt-in” are met. The conditions of the soft opt-in are that: (i) the person marketing has obtained the relevant individual’s details in the course of selling or negotiating a sale of products or services offered by such person; (ii) the direct marketing only markets the same person’s similar products and services; (iii) the individual was given the opportunity to opt out of marketing when their details were first collected but did not opt out at that point; and (iv) the individual is given the opportunity to opt out on each subsequent marketing communication.
- All consent requirements under the UCR can currently be validly obtained by either opt-in or opt-out consent.

The Regulations provide that the ICO will issue a direct marketing Code to contain practical guidance in relation to the carrying out of direct marketing in accordance with the requirements of the data protection legislation. This Code has not yet been made available.

9.2 Please describe any legislative restrictions on the sending of direct marketing communications via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance, for marketing by post, there are no consent or opt-out requirements, etc.).

The following provisions apply:

- Direct marketing activities must generally comply with the Regulations and the applied GDPR, and direct marketing communicated by telephone calls or faxes must comply with the UCR.
- Direct marketing by post is not subject to specific regulation, but any processing of personal data for the purpose of direct marketing must be done in compliance with the principles of the Regulations and the applied GDPR.
- Persons marketing by way of live telephone calls may not make unsolicited calls if either: (i) the individual or corporation contacted has previously notified the person marketing that such calls should not be made to such individual’s or corporation’s telephone number; or (ii) the telephone number is listed on the register provided by the UK Telephone Preference Service (“TPS”) (to whom the responsibility of maintaining the Isle of Man register has been delegated).
- Automated telephone marketing calls may only be made with the consent of the individual or corporation to whom such calls are directed.

The Regulations provide that the ICO will issue a direct marketing Code to contain practical guidance in relation to the carrying out of direct marketing in accordance with the requirements of the data protection legislation. This Code has not yet been made available.
9.3 Do the restrictions noted above apply to marketing sent from other jurisdictions?

The restrictions would only apply to marketing sent from the Island.

9.4 Is/are the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?

The ICO has a range of powers under the Regulations and the applied GDPR where breaches of marketing restrictions were due to data protection issues.

9.5 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?

There is no legal restriction to prevent the purchase of marketing lists from third parties. A data controller would, however, have to give serious consideration to the origin of the list and the data subject’s awareness that their data has been sold in this way in order to ensure compliance with the data protection requirements.

9.6 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?

There are no specific penalties set out in the current law. A person suffering damage by reason of contravention of the law is entitled to bring proceedings for financial compensation against the person contravening the law.

10 Cookies

10.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).

The UCR implemented Article 13 of the European Privacy and Electronic Communications Directive (2002/58/EC) (“Privacy Directive”). The UCR have not yet been amended to incorporate the changes made to the Privacy Directive regarding cookies in May 2011. As a result, the requirements of the Privacy Directive are regarded as “best practice” only on the Isle of Man, and implementation of the guidance relating to cookies remains voluntary.

10.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?

As above, there is no specific legislation or binding guidance regarding cookies on the Isle of Man.

10.3 To date, has/have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?

There is no evidence that the ICO has taken any enforcement action in relation to cookies.

10.4 What are the maximum penalties for breaches of applicable cookie restrictions?

There are no relevant penalties.

11 Restrictions on International Data Transfers

11.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.

Under the Regulations and applied GDPR, data transfers to a third country can only take place if the transfer is to an “Adequate Jurisdiction” (as specified by the EU Commission) or approval has been obtained from the ICO in respect of any measures which the data controller is proposing to take in accordance with the applied GDPR. A third country is defined as a State, territory or jurisdiction other than the Isle of Man and which is not a Member State of the European Union. The Isle of Man Parliament has recently (March 2019) approved the Data Protection (Withdrawal from the EU) (UK and Gibraltar) Regulations 2019, which will enable data transfers to both territories to continue without additional safeguards post-Brexit.

11.2 Please describe the mechanisms businesses typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).

Subject to approval from the ICO, when transferring personal data to a third country, businesses must ensure that there are appropriate safeguards on the data transfer, as prescribed by the applied GDPR. The applied GDPR offers a number of ways to ensure compliance for international data transfers, of which one is consent of the relevant data subject. Other common options are the use of Standard Contractual Clauses or Binding Corporate Rules (“BCRs”). Businesses can adopt the Standard Contractual Clauses drafted by the EU Commission – these are available for transfers between controllers, and transfers between a controller (as exporter) and a processor (as importer). International data transfers may also take place on the basis of contracts agreed between the data exporter and data importer, provided that they conform to the protections outlined in the applied GDPR, and they have prior approval by the relevant data protection authority.

International data transfers within a group of businesses can be safeguarded by the implementation of BCRs. The BCRs will always need approval from the relevant data protection authority. Most importantly, the BCRs will need to include a mechanism to ensure they are legally binding and enforced by every member in the group of businesses. Among other things, the BCRs must set out the group structure of the businesses, the proposed data transfers and their purpose, the rights of data subjects, the mechanisms that will be implemented to ensure compliance with the GDPR, and the relevant compliant procedures.

Transfer of personal data to the US is also possible if the data importer has signed up to the EU-US Privacy Shield Framework, which was designed by the US Department of Commerce and the EU Commission to provide businesses in the EU and the US with a mechanism to comply with data protection requirements when transferring personal data from the EU to the US.
The Isle of Man Parliament has recently (March 2019) approved the Data Protection (Withdrawal from the EU) (UK and Gibraltar) Regulations 2019, which will enable data transfers to both countries to continue without additional safeguards post-Brexit.

11.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.

Under the applied GDPR, the ICO has to approve any transfer of personal data to a third country which is not subject to an adequacy decision.

12 Whistle-blower Hotlines

12.1 What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?

There is no reference to whistle-blowing within the data protection law or regulations. Normal standards of data protection would be expected to apply to any data processed as a result of operating such a hotline.

12.2 Is anonymous reporting prohibited, strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do businesses typically address this issue?

There is no reference to whistle-blowing within the data protection law or regulations and so there are no restrictions around anonymous reporting. Generally, regulatory and government guidance on whistle-blowing encourages the reporter to disclose their name to assist in investigations.

13 CCTV

13.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?

Prior approval is not required from the ICO to use CCTV. A separate notification is also not required. The ICO’s guidance recommends the use of clear and visible signage, which includes who to contact about the operation of the CCTV system.

13.2 Are there limits on the purposes for which CCTV data may be used?

The ICO’s guidance states that there must be a lawful reason for considering the use of CCTV which cannot be met in another way. The ICO also suggests that the appropriateness for use of CCTV should be kept under review. Cameras should not be installed in private areas unless there are exceptional circumstances.

14 Employee Monitoring

14.1 What types of employee monitoring are permitted (if any), and in what circumstances?

Employee monitoring is permitted, provided that compliance with the data protection legislation is achieved. Monitoring must be proportionate to the intended aim, not adversely impact the privacy of the individuals, and be justified by its benefit to the employer. It would generally be viewed as unfair to tell employees that monitoring is being undertaken for one purpose and then use the information obtained for another purpose.

14.2 Is consent or notice required? Describe how employers typically obtain consent or provide notice.

Employers are required, on an ongoing basis, to make employees aware of any monitoring which is undertaken and the reasons for it, except in the exceptional limited circumstances where covert monitoring is necessary. Consent would only be required where an employer needed to rely on it as a legitimising condition for the processing of the personal data in accordance with the data protection legislation. Employers typically provide notice through a range of measures such as inclusion in the staff handbook, notices in the workplace and regular reminders through formal and informal communications. Employers typically obtain consent through clear and specific fair processing notices signed by the employees.

14.3 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?

There is no requirement for such representatives to be notified or consulted.

15 Data Security and Data Breach

15.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?

Yes. Personal data must be processed in a way which ensures security and safeguards against unauthorised or unlawful processing, accidental loss, destruction and damage of the data. Both controllers and processors must ensure they have appropriate technical and organisational measures to meet the requirements of the data protection legislation. Depending on the security risk, this may include the encryption of personal data, the ability to ensure the ongoing confidentiality, integrity and resilience of processing systems, an ability to restore access to data following a technical or physical incident, and a process for regularly testing and evaluating the technical and organisational measures for ensuring the security of processing.
15.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

The controller is responsible for reporting a personal data breach without undue delay (and in any case within 72 hours of first becoming aware of the breach) to the relevant data protection authority, unless the breach is unlikely to result in a risk to the rights and freedoms of the data subject(s). A processor must notify any data breach to the controller without undue delay.

The notification must include the nature of the personal data breach, including the categories and number of data subjects concerned, the name and contact details of the Data Protection Officer or relevant point of contact, the likely consequences of the breach and the measures taken to address the breach, including attempts to mitigate possible adverse effects.

15.3 Is there a legal requirement to report data breaches to affected data subjects? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

Controllers have a legal requirement to communicate the breach to the data subject, without undue delay, if the breach is likely to result in a high risk to the rights and freedoms of the data subject.

The notification must include the name and contact details of the Data Protection Officer (or point of contact), the likely consequences of the breach and any measures taken to remedy or mitigate the breach.

The controller may be exempt from notifying the data subject if the risk of harm is remote (e.g., because the affected data is encrypted), the controller has taken measures to minimise the risk of harm (e.g., suspending affected accounts) or the notification requires a disproportionate effort (e.g., a public notice of the breach).

15.4 What are the maximum penalties for data security breaches?

The proposed revised law contains a maximum discretionary penalty of up to £1 million for breaches which are other than those prescribed in the GDPR.

16 Enforcement and Sanctions

16.1 Describe the enforcement powers of the data protection authority(ies).

<table>
<thead>
<tr>
<th>Investigatory Power</th>
<th>Civil/Administrative Sanction</th>
<th>Criminal Sanction</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information Notice – requires a controller or processor to provide the ICO with the information that the reasonably requires.</td>
<td>On summary conviction, a fine not exceeding level 5 on the standard scale or to custody of not more than six months or both. On conviction on information, an unlimited fine.</td>
<td>Not applicable.</td>
</tr>
</tbody>
</table>

16.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?

The Regulations entitle the ICO to impose a temporary or definitive limitation, including a ban on processing.

16.3 Describe the data protection authority’s approach to exercising those powers, with examples of recent cases.

Enforcement to date has been limited to Enforcement Notices and Formal Undertakings against Isle of Man data controllers.

16.4 Does the data protection authority ever exercise its powers against businesses established in other jurisdictions? If so, how is this enforced?

Enforcement to date has been limited to Enforcement Notices and Formal Undertakings against Isle of Man data controllers.

17 E-discovery / Disclosure to Foreign Law Enforcement Agencies

17.1 How do businesses typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?

The duty of confidentiality and compliance with the data protection principles would be uppermost in the minds of companies responding to such requests. Traditionally, the obligation to exchange information, such as under automatic exchange of information regimes, would be covered in an organisation’s terms and conditions. For data protection reasons, though, exchange of information is often limited to Isle of Man statutory or public authorities, rather than data being released to foreign authorities. Isle of Man companies are very mindful of requests from foreign law enforcement agencies, and would be keen to ensure that these have come through the appropriate channels in advance of replying to them.

17.2 What guidance has/have the data protection authority(ies) issued?

There is no specific guidance in this area.
18 Trends and Developments

18.1 What enforcement trends have emerged during the previous 12 months? Describe any relevant case law.

The ICO’s website lists four Enforcement Notices served from 2012 to date. These relate to (i) the processing of personal data from surveillance equipment on buses without the appropriate signage, (ii) the sending of direct marketing by email without proper regard for data protection and other regulatory requirements, (iii) matters connected to (i), and (iv) proper compliance with the right of data subject access. Two formal undertakings were also issued in 2017 relating to a data subject access request and the improper publication of personal data.

18.2 What “hot topics” are currently a focus for the data protection regulator?

The ICO is focused on publishing guidance and resources to assist data controllers and processors to comply with the Regulations and applied GDPR.

Sinead O’Connor is DQ’s Head of Regulatory & Compliance Services and is a member of the Data Protection Team. Sinead advises clients on the regulatory and compliance aspects of data protection and the GDPR, in particular on the implications of the GDPR for data retention and on the general impact on data protection policies. Sinead, who is a qualified data protection practitioner, regularly delivers training to Boards of Directors and senior management on the practical implications of current data protection legislation and the GDPR.

Adam Killip is a senior associate within the corporate & commercial and regulatory and compliance departments. Adam’s practice encompasses a broad range of corporate, commercial and regulatory work, including corporate acquisitions and sales, banking and finance transactions, shareholder disputes and insolvency matters. From a regulatory perspective, Adam regularly advises clients on their legal obligations under financial services legislation, and has experience assisting clients with enforcement action being taken by the financial services regulator. Adam also advises on data protection queries and is an accredited Data Protection Practitioner.

DQ Advocates is a leading Isle of Man-based law firm with an international reach. We offer a full range of legal, regulatory and compliance services to our local and global clients. DQ are accessible, responsive and commercial with client-oriented strategies and goals. Our specialist lawyers are recommended as leading lawyers in Chambers & Partners and The Legal 500.
1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

The principal legislation is the Protection of Privacy Law, 5741-1981 ("PPL") and the regulations enacted thereunder; in particular, the Protection of Privacy Regulations (Data Security), 5777-2017 ("Security Regulations").

1.2 Is there any other general legislation that impacts data protection?


1.3 Is there any sector-specific legislation that impacts data protection?

Yes. The Credit Data Law, 5776-2016 governs the credit data sharing centrally maintained by the Bank of Israel. The Inclusion of Biometric Identifiable Means and Information in Identifying Documentation and Database, 5770-2009 governs, inter alia, data protection with respect to Israel’s national biometric database of Israeli citizens. Other notable sectors are the health, banking, finance and insurance sectors with respect to which regulatory requirements are set out under specific directives and circulars issued by the respective regulators.

1.4 What authority(ies) are responsible for data protection?

The Protection of Privacy Authority (formerly known as ILITA) ("PPA"). The PPA serves as, inter alia, Israel’s data protection authority (for both the private and public sectors). As a data protection regulator, the PPA serves as the Registrar of Databases ("Registrar"), which is responsible for data protection regulation and enforcement. Its powers include complaint handling, investigation of offences, imposition of fines, registration of computerised databases, issuing compliance instructions, setting guidelines and standard codes of practice, etc.

2 Definitions

2.1 Please provide the key definitions used in the relevant legislation:

- **Personal Data**
  Information about an individual’s personality, personal status, intimate affairs, health condition, financial condition, professional qualifications, opinions and beliefs (defined under the PPL as "Information").

- **Processing**
  Includes disclosure, transfer and delivery (defined under the PPL as "Use").

- **Controller**
  The person or entity which is responsible for the collection of personal data, the means by which and the purposes for which the personal data will be collected and processed (referred to as the "Owner of a Database").

- **Processor**
  The PPL does not define "Processor" but refers to a "Holder" of a Database, which is defined as a person who has a database in his possession on a permanent basis and is permitted to use it.

- **Data Subject**
  There is no formal definition under the PPL, but it is viewed as any natural person about whom Information or Sensitive Information is included in a Database.

- **Sensitive Personal Data**
  Information on a person’s personality, intimate (i.e. private) affairs, state of health, financial conditions, opinions and beliefs; information that the Minister of Justice determined by order, with the approval of the Constitution, Law and Justice Committee of the Knesset, is sensitive (defined under the PPL as "Sensitive Information").

- **Data Breach**
  An event where Information from the Database was used without authorisation or in breach of an authorisation or where harm was caused to the integrity of the information (defined under the Security Regulations as a "Severe Security Incident").

Other key definitions – please specify (e.g., “Pseudonymous Data”, “Direct Personal Data”, “Indirect Personal Data”)

- **Consent**
  Informed, express or implied.

- **Database**
  A collection of Information, maintained by magnetic or optical means and intended for computer processing, excluding: (i) a
non-business collection of Information; and (ii) a collection that includes only names, addresses and means of communicating, which by themselves do not create any characteristics that infringe on the privacy of individuals whose names are included on it, on the condition that neither the owner of the collection, nor a body corporate under its control, owns an additional collection.

- **Manager of a Database**
  An active manager of a body that owns or possesses a Database or a person whom the aforesaid manager authorised for this purpose.

- **Public Body**
  (1) a governmental department and any other state institution, local authority and any other body carrying out public functions under any law; or (2) a body designated by the Minister of Justice by order, with the approval of the Constitution, Law and Justice Committee of the Knesset.

- **Direct Mailing**
  Approaching a specific person based on his belonging to a group of the population that is determined by one or more characteristics of persons whose names are included in a Database.

- **Direct Mailing Services**
  Providing Direct Mailing Services, by way of transferring lists, labels or data to others by any means.

### 3 Territorial Scope

#### 3.1 Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to those laws?

The PPL has no specific reference to its territorial scope. To date, the question as to whether Israeli privacy laws apply to foreign entities without any presence in Israel has not yet been addressed by the Israeli courts or the PPA. However, as a common perception, it is likely that they will apply, based on certain linkages of these to Israel, including: (i) if servers containing personal data are located in Israel; (ii) if the controller of the personal data is Israeli or based in Israel; (iii) if processing activities are conducted in Israel; or (iv) if there are Israeli data subjects.

### 4 Key Principles

#### 4.1 What are the key principles that apply to the processing of personal data?

- **Transparency**
  The PPL stipulates (Section 11) that any request made to a person for personal data, with the intention to keep and use it in a Database, shall be accompanied by a notice indicating: (i) whether there is legal obligation to deliver the data or whether the delivery is based on free will and consent; (ii) the purpose for which the data is requested; and (iii) to whom will the data be delivered and for what purpose. Under the PPL (Section 17F), in any Direct Mailing approach, individuals must also be informed about their right to request deletion of data from the Database.

- **Lawful basis for processing**
  See under “Transparency” above. The PPL does not address the matter of ‘processing’; however, it is presumed to be included under the definition of “Use”. The PPL stipulates (Section 8(a)) that managing or holding a Database which is required to be registered with the Registrar must be registered.

- **Purpose limitation**
  No person shall use data included in a Database other than for the purpose for which the Database was registered (Section 8(b) to the PPL). Using, or passing onto another, information on a person’s private affairs otherwise than for the purpose for which it was given, constitutes an infringement of privacy (Section 2(9) to the PPL).

- **Data minimisation**
  Section 2(c) of the Security Regulations states that an Owner of a Database shall annually assess whether the data he is keeping in the Database is more than necessary for the objectives of the Database.

- **Proportionality**
  Violation of the right to privacy shall not be greater than is required (Section 8 to the Basic Law). The principle of proportionality was adopted in the PPA’s guidelines with respect to CCTV data (4/2012 and 5/2017) and candidates’ data (2/2012), and by the Israeli courts with respect to the use of employees’ biometric data (the Qalanswa case).

- **Retention**
  The PPL does not specifically address this matter, however the interpretation of the PPA (guidelines 2/2012) is that personal data only for the necessary period in order to fulfil the applicable purpose for which the data was collected. According to Section 2(c) to the Security Regulations, an Owner of a Database must review, on an annual basis, that personal data maintained by it in a Database is not in excess of what is required in order to fulfil the purposes of the Database. Under the Security Regulations and the PPA’s guidelines regarding outsourcing (2/2011), when personal data is processed by an external entity, the Owner of a Database must ensure that the data will be deleted (except in certain circumstances) following the completion of services.

#### Other key principles – please specify

This is not applicable.

### 5 Individual Rights

#### 5.1 What are the key rights that individuals have in relation to the processing of their personal data?

- **Right of access to data/copies of data**
  Under the PPL (Section 13), data subjects have the right to access data about them that is stored in a Database. This right applies to data in any form and format (PPA’s guidelines 1/2017). In instances where data is not held by the Owner of the Database but by a Holder, the Owner must provide the data subject with the contact details of the Holder, and order the Holder, in writing, to provide access to the Data requested. There are some exceptions to the right of access: if the data may cause serious harm to the data subject’s physical or mental health; if access may cause the violation of a privilege under law; and if the Database is maintained by certain public authorities.

- **Right to rectification of errors**
  The PPL determines (Section 14) that data subjects may request correction or deletion of personal data that is incorrect, incomplete, unclear, or not up to date. If a request is approved, the Owner must correct or delete the data. In case a request is rejected, the applicant is entitled to appeal to a competent court.
6 Registration Formalities and Prior Approval

6.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?

Under the PPL (Section 8(c)), a Database must be registered if any of the following applies:

(i) the Database contains Information about more than 10,000 individuals;
(ii) the Database contains Sensitive Information;
(iii) the Database contains Information about persons and the Information was not provided to the Database by them, on their behalf, or with their consent;
(iv) the Database belongs to a Public Body; and
(v) the Database is used for Direct Mailing Services.

6.2 If such registration/notification is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?

The application must be specific, and all processing activities and categories of data processed must be disclosed.

6.3 On what basis are registrations/notifications made (e.g., per legal entity, per processing purpose, per data category, per system or database)?

Registration is made per Database (which can be a combination of IT systems) and per processing purpose.

6.4 Who must register with/notify the data protection authority (e.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation)?

The Owner of the Database, regardless of its identity (i.e. whether local or foreign, private or public entity).

6.5 What information must be included in the registration/notification (e.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes)?

The application must specify, inter alia:

(i) the identities of the Owner of the Database, the Holder(s) of the Database, and the Manager of the Database and their addresses in Israel;
(ii) the purposes for which the Database is established;
(iii) types of Information included in the Database;
(iv) the manner of, and legal basis for collection;
(v) details regarding transfer of Information to third parties; etc.

Additional information and documents can be requested by the Registrar.

6.6 What are the sanctions for failure to register/notify where required?

Under the PPL (Section 31A(a)), failure to register a Database constitutes a criminal offence punishable by a year’s imprisonment. The PPA may impose fines (up to NIS 2,000 for individuals and NIS 10,000 for corporate entities).

6.7 What is the fee per registration/notification (if applicable)?

This is not applicable.

6.8 How frequently must registrations/notifications be renewed (if applicable)?

Under the PPL (Section 9(d)), updating the Registry is required upon certain changes (e.g. with respect to the identity of the Owner/Holder/Manager of the Database, the purposes of the Database, types of Information included in the Database, etc.) or in the event of discontinuance of the operation of the Database (in which case the Database must be deleted from the Registry).

6.9 Is any prior approval required from the data protection regulator?

Yes. Data included in a Database may be processed only where the Database is registered in the Registry (Section 8(a) of the PPL). Under the PPL (Section 10), if there is no response from the Registrar within 90 days from filing, then using the Database is permitted even without registration.

6.10 Can the registration/notification be completed online?

Yes, online registration/notification is possible.
6.11 Is there a publicly available list of completed registrations/notifications?

Yes; however, only partial information regarding registered databases is available. The original applications are non-public.

6.12 How long does a typical registration/notification process take?

This usually takes a few days to a few weeks.

7 Appointment of a Data Protection Officer

7.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.

Yes, with respect to the following entities (Section 17B to the PPL): an entity that holds five or more databases that require registration; Public Bodies and banks; insurance companies; and companies engaged in ranking or evaluating credit ratings.

According to the PPA’s guidelines for outsourcing, in any engagement for outsourcing services involving the processing of personal data, it is recommended that both the entity ordering the services and the service provider appoint a DPO.

7.2 What are the sanctions for failing to appoint a Data Protection Officer where required?

Failure to appoint a DPO constitutes a criminal offence punishable by a year’s imprisonment (Section 31A(a) of the PPL). The PPA may impose fines (up to NIS 3,000 for individuals and NIS 15,000 for corporate entities).

7.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect of his or her role as a Data Protection Officer?

No, the Data Protection Officer is not protected from disciplinary measures and other employment consequences.

7.4 Can a business appoint a single Data Protection Officer to cover multiple entities?

Yes, provided that the DPO is granted the resources necessary to carry out its role and does not undertake any other role that could pose a conflict of interest.

7.5 Please describe any specific qualifications for the Data Protection Officer required by law.

The DPO must be a person with competent training and cannot be a person previously convicted of a flagrant offence or in an offence under the Privacy Law (Section 17B of the PPL).

7.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?

The DPO is responsible for: (i) the security of the Databases (Section 17B to the PPL); and (ii) to prepare (a) a data security procedure for the Databases and bring it to the Owner of the Database for approval, and (b) a plan for the ongoing audit of compliance with the requirements of the Security Regulations, to perform it and to notify the Owner and Manager of the Database of its findings (Sections 3(2) – (3) of the Security Regulations).

7.7 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?

Yes, in the application for the registration of a Database and in an annual report which a holder of five or more Databases that require registration must file to the Registrar (Section 17A(b) of the PPL).

7.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?

No, the Data Protection Officer does not need to be named in a public-facing privacy notice or in an equivalent document.

8 Appointment of Processors

8.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?

Yes. The PPA’s outsourcing guidelines (2/2011) require that an agreement be entered into between the Owner of the Database and the service provider who processes Personal Data on its behalf. In addition, under the Security Regulations (Section 15), the Owner of the Database must enter into an agreement with any external service provider involving the grant of access to a Database. This type of agreement is also required in the banking, financial services and insurance sectors.

8.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?

There are no formalities, but it is common to have a written agreement in place. This type of agreement should include the following:

i) processing of personal data only for the purpose for which the data was provided;

ii) description of the types of data processed;

iii) security of the personal data;

iv) the duration of the agreement, and arrangement and deletion of data upon termination of the agreement; and

v) the use of sub-processors and their protection of the personal data, audit rights and reporting obligation (including in cases of data breaches), etc.
9 Marketing

9.1 Please describe any legislative restrictions on the sending of electronic direct marketing (e.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?).

Section 30A of the Communications Law (Bezeq and Transmissions), 5742-1982 (“Spam Law”) prohibits the sending of marketing material (including propaganda and requests for donations) to recipients by automated means (e.g., email, automated telephone message, facsimile or SMS), unless: (i) the recipient has granted his explicit prior written (including by email or a recorded call) consent (although a one-time message to a business client requesting consent for marketing is permitted), or (ii) the recipient has given his details in the past to the advertiser in connection with the purchase of a similar service/product and the advertiser has informed him that the details would be used for marketing, and the recipient has been given the opportunity to decline to receive such marketing. Any marketing message must (1) clarify that it is a marketing message, (2) include the advertiser’s contact details, and (3) inform the recipient of his right to decline to receive such marketing in the future and provide an address to which the recipient may deliver such notice.

The PPL regulates the matter of Direct Mailing that applies to any type of marketing executed in any media and form. In addition to the requirements under the Spam Law, if applicable, any Direct Mailing must include: the registration number of the Database used for the Direct Mailing Services; the identity and address of the Owner of the Database; and the sources from which it received the Data Subject’s details.

9.2 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.).

The Spam Law applies only to the automated means specified in our previous response. Sending of marketing via other means is not subject to any special restrictions, unless such communication is considered a “Direct Mailing” (as detailed above).

9.3 Do the restrictions noted above apply to marketing sent from other jurisdictions?

Yes, however enforcement may be challenging.

9.4 Is/are the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?

The PPA is responsible for enforcement of violations relating to Direct Mailing. There is no responsible authority for violations of the Spam Law.

9.5 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?

Yes. The PPA published some “rules of thumb” for all those considering acquiring databases, in order to ascertain the validity of the transaction. These include the receipt of the seller’s confirmation that it complies with the provisions of the PPL, verifying that the purchased database has been registered, that the seller lawfully collected the data and that it maintains a list of sources of such data, etc.

9.6 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?

For violating the provisions of the PPL with respect to Direct Mailing – an administrative fine of up to NIS 3,000 (or NIS 15,000 for corporate entities). For violating the provisions of the Spam Law – a criminal fine of up to NIS 226,000 and statutory damages of up to NIS1,000 per message. Each of the above violations constitutes a civil tort as well.

10 Cookies

10.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).

There is no specific legislation pertaining the use of cookies. The PPA issued (non-binding) recommendations for organisations operating websites, advising them to make a privacy policy available, which, inter alia, details the tracking tools used in the website (e.g. cookies), their purposes and whether the website permits third parties to use tracking tools and for what purposes.

10.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?

This is not applicable.

10.3 To date, has/have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?

No such action has been taken to date.

10.4 What are the maximum penalties for breaches of applicable cookie restrictions?

This is not applicable.

11 Restrictions on International Data Transfers

11.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.

The Protection of Privacy Regulations (The Transfer of Data to a Database outside the State Borders), 5761-2001 (the “Transfer Regulations”) permit the transfer of personal data from a database in Israel to a database located outside of Israel, provided the law in the receiving country provides a level of protection of personal data not lower than that provided for under the Israeli law, including, in certain circumstances (not an exhaustive list):

i) with the consent of the affected data subject;

ii) when data is being transferred to a corporation controlled by the Owner of the Database and it has ensured the protection of privacy following the transfer;
iii) when the recipient has undertaken an agreement with the Owner of the Database to comply with Israeli privacy laws; and

iv) when data is being transferred to a database in a country which is a party to the European Convention for the Protection of Individuals with Regard to Automatic Processing of Sensitive Data or in a country which receives data from Member States of the European Union, under the same conditions of receipt.

In addition, the owner of the Israeli Database must ensure (via written agreement with the recipient) that the recipient is taking adequate measures to ensure the privacy of data subjects and that the data will not be further transferred.

### 11.2 Please describe the mechanisms businesses typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).

Israeli businesses typically rely on the following:

i) consent of a data subject; transfer to a third party in an EU Member State; and

ii) transfer to a third party who has undertaken to comply with Israeli privacy laws.

### 11.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.

Yes, as registration of a database requires the disclosure of any transfer of personal data to third parties (including non-Israelis). Owners must also update a registration when a new transfer of data outside of Israel is exercised.

### 12 Whistle-blower Hotlines

#### 12.1 What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?

Israeli law does not address this issue, and general Israeli data protection and employment laws would apply.

#### 12.2 Is anonymous reporting prohibited, strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do businesses typically address this issue?

It is generally permitted.

### 13 CCTV

#### 13.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?

According to the PPA’s guidelines, database registration/notification or prior approval from the relevant data protection authority(ies) is required for CCTV data collection.

#### 13.2 Are there limits on the purposes for which CCTV data may be used?

CCTV footage must only be used for the purpose for which it was originally collected. Under the CCTV guidelines, the impact of the use of CCTV on privacy must be evaluated against less intrusive alternatives, in order to achieve the purpose. Careful scrutiny should be applied when using CCTV in areas of minors, when using special functionalities (e.g., face recognition), or when using CCTV in the workplace (see below).

### 14 Employee Monitoring

#### 14.1 What types of employee monitoring are permitted (if any), and in what circumstances?

Employee monitoring is generally permitted, subject to the following principles.

In 2011, the Israeli National Labour Court set a major precedent (the Isakov case) as to the boundaries of the employer’s ability to infiltrate its employees’ professional mailbox (and other workplace computer systems). The Court ruled that monitoring must be legitimate (and limited to essential business purposes), proportionate (means which are the least harmful to the employees’ privacy must be used), limited only to what is necessary in order to achieve the initial purpose and transparent (a clear policy regarding the monitoring must be brought to the employees’ attention and they must consent to it). Infiltration of personal correspondence should only occur in exceptional circumstances, where protecting the employer’s legitimate interests would justify the employee’s privacy violation. The employee’s explicit and informed consent with respect to accessing specific personal email correspondence is required. The employer is
forbidden from monitoring an employee’s use of a private mailbox, without a court order.

In addition, under the PPA’s guidelines with respect to the use of surveillance cameras in the workplace (5/2017), installation of surveillance cameras in the workplace should be made only for legitimate purposes, employees’ explicit consent for the use of the cameras must be obtained, a clear and detailed policy regarding the use of the cameras must be presented to the employees, private areas will not be covered, and the use of footage for purposes which are different from the purpose which has been pre-determined is prohibited.

Furthermore, in 2017, the Israeli National Labour Court ruled (the Qalansawa Municipality case) that the use of a biometric system for monitoring attendance harms the employees’ right to privacy and their right to autonomy, and consequently, an employer’s right will only triumph above its employees’ right to privacy if required by law or with the employees’ free-willed and specific consent.

14.2 Is consent or notice required? Describe how employers typically obtain consent or provide notice.

Israeli case law mandates explicit consent of employees to any infringement of their right to privacy, due to the unbalanced employer-employee relationship. Consent must be informed and free-willed, and it is usually obtained through the employment agreement or specific policies which are made available to the employees and they are required to consent to them.

14.3 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?

There are no specific statutory requirements in this regard. Under Israeli case law, consultation with employee representatives is obligatory whenever the rights of employees may be affected. Under the PPA’s guidelines relating to CCTV in the workplace (5/2017), the employer should establish a policy regarding the use of cameras in the workplace after consulting with the employees or their representatives.

15 Data Security and Data Breach

15.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?

Section 17 to the PPL stipulates that the Owner, Holder and Manager of a Database are each responsible for the protection of the data in the Database. The Security Regulations set out data security controls and measures that must be applied, depending on the level of sensitivity of the data, number of data subjects and number of individuals with access rights. These include controls relating to physical and environmental security, performance of security risk surveys and penetration tests, access permissions management, security event documentation and reporting, use of mobile devices, communication security, outsourcing to third parties, backup and recovery, etc.

15.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

The Security Regulations (Section 11) provide that an Owner or a Holder of the Database must notify the Registrar in case of a Severe Security Incident and send a report to the Registrar with respect to the steps taken as a result of the event. According to the PPA’s guidelines, notification to the Registrar shall take place within 24 hours of becoming aware of the event and in any case no later than 72 hours as of such date.

Notification to the Registrar can be made online and must include details of the Owner and Manager of the Database, number of the registered Database, details regarding the event (e.g. date of the event, how it was discovered, how it happened, measures in place to prevent such events), types of personal data affected or at risk, negative impact on the affected data subjects, measures implemented for recovery, mitigation of the effect of the event on affected data subjects and prevention of recurrence of similar events, reporting to the relevant authorities, etc.

15.3 Is there a legal requirement to report data breaches to affected data subjects? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

Only if the Registrar instructs the Owner to notify data subjects, following a consultation with the national cybersecurity authority.

15.4 What are the maximum penalties for data security breaches?

To date, data security breaches are not subject to either criminal or administrative penalties.

16 Enforcement and Sanctions

16.1 Describe the enforcement powers of the data protection authority(ies).

<table>
<thead>
<tr>
<th>Investigatory Power</th>
<th>Civil/Administrative Sanction</th>
<th>Criminal Sanction</th>
</tr>
</thead>
<tbody>
<tr>
<td>Request for information and documents pertaining to a Database</td>
<td>Under the Administrative Offences Regulations (Administrative Fine – Protection of Privacy), 5764 – 2004, the PPA may impose administrative fines for violations of the PPL, ranging from NIS 2,000 – NIS 5,000 (and up to five times these amounts if the violation is conducted by a corporate entity). One-tenth of the fine may be imposed for each day of the occurring violation.</td>
<td>Criminal investigatory powers. The PPA usually forwards its findings to the State Attorney for prosecution.</td>
</tr>
<tr>
<td>Audits</td>
<td>Postponement or cancellation of a Database registration.</td>
<td>N/A</td>
</tr>
</tbody>
</table>
16.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?

In case of any violation of the PPL or any order issued by the Registrar, the Registrar may postpone or cancel a registration of a database (without any court order).

16.3 Describe the data protection authority’s approach to exercising those powers, with examples of recent cases.

The PPA is very active, though criminal fines are reserved for severe cases of breach of the PPL.

In 2017, the PPA initiated a criminal investigation (the “Good People” case), which involved the unlawful transfer of the personal data of pregnant women intending to carry out abortions from a medical clinic to a non-profit, anti-abortion organisation. Upon completion of the investigation, the case was referred to the State Attorney’s Cyber Department, which filed an indictment against the individuals involved in March 2018.

According to the publicly available information on the PPA’s website, in 2018 there were 13 cases in which the PPA imposed administrative sanctions (including fines and publication of a breach of the PPL by the infringing party) with respect to violations of the Privacy Law.

In July 2018, the PPA imposed administrative fines (NIS 60,000) on a company (Ambulanel) that provides emergency medical services, for the unlawful use of a stolen governmental database and for not registering its databases.

In June 2018, the PPA imposed administrative fines (NIS 25,000) on the National Teachers’ Organisation (Histadrut Ha’morim L’Israel) that has used a database other than for the purpose for which it was established and failed to comply with the provisions of the Security Regulations.

In January 2018, the PPA imposed administrative fines (NIS 100,000) on a financial services company (Livne Dani) providing financial debt services, for the unlawful use of governmental databases.

16.4 Does the data protection authority ever exercise its powers against businesses established in other jurisdictions? If so, how is this enforced?

No, it does not exercise such powers.

17 E-discovery / Disclosure to Foreign Law Enforcement Agencies

17.1 How do businesses typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?

There are no specific requirements in this regard, and businesses should comply subject to the provisions of the PPL, including the Transfer Regulations. The Legal Assistance between Countries Law, 5758-1998, which applies, inter alia, to the transmittal of evidence and other documents in connection with a civil or a criminal matter, provides for an alternative route for exchanging information between countries or certain specified bodies set out under such law, which is not necessarily related to privacy issues.

17.2 What guidance has/have the data protection authority(ies) issued?

This is not applicable.

18 Trends and Developments

18.1 What enforcement trends have emerged during the previous 12 months? Describe any relevant case law.

In August 2018, the PPA announced that a new inspection unit had been added to the criminal and administrative enforcement agencies of the PPA. According to the PPA’s announcement, the new unit will perform a cross-sectoral inspection in order to examine the implementation of the provisions of the PPL and the regulations enacted thereunder, at all levels of the Israeli economy, on a sectoral and thematic basis.

As of 2018, there is a growing trend on the part of the PPA to initiate investigative proceedings and take a more active approach following events that receive media coverage and which raise questions or concerns about privacy and data security laws. As part of these investigative proceedings, the PPA investigates both the event itself as well as the general data collection, analysis and security procedures in place within the affected organisation.

18.2 What “hot topics” are currently a focus for the data protection regulator?

In February 2018, a proposed amendment to the PPL was approved by the Israeli government and is currently pending before the Israeli Parliament. The purpose of the amendment is to enhance the Israeli PPA’s supervision and enforcement authority with respect to the Privacy Law and its violations. If passed, the Registrar will be vested with increased investigative powers and the ability to impose greater monetary fines of up to NIS 3.2 million. The legislation is currently gridlocked.

On February 2017, a non-governmental draft bill initiated by several members of the Israeli Parliament was issued, titled “The Draft Bill Protection of Privacy Law (Amendment – Protection of Privacy of Minors), 2017”. The bill aims to determine stricter rules regarding the collection and use of personal information pertaining to minors. The legislation is currently gridlocked.

In addition, in a unique seminar held jointly by the Israeli Bar Association and the Israeli Democracy Institute, an NGO that serves as an independent centre of research and action (the “IDI”) in January 2019, a proposed draft bill to amend the PPL was presented by the IDI (the “Bill”). The Bill, which is a private initiative, aims to close the ever-growing gaps between the current privacy legislation in Israel and the GDPR and, in this respect, the provisions of the Bill bear a striking resemblance to those of the GDPR. In this regard, the Bill includes a proposal to apply an extraterritorial scope to the Israeli privacy legislation, to repeal the mandatory registration of databases, to establish additional legitimate bases for processing, to
redefine sensitive data (the processing of which will be subject to express written consent), to propose a special mechanism for dealing with the personal data of minors, to expand data subjects’ rights, to propose the regulation of automated processing, to introduce the right to deletion, and to strengthen the powers and status of the PPA.

On 28 January 2019, the PPA announced that the “grace period” granted to organisations to comply with the requirements under the Security Regulations has ended and that from now on, the PPA will strengthen its enforcement with respect to any violations of the Data Security Regulations.

Ohad Elkeslassy is a partner in HFN’s Commercial Clients Department with diverse and extensive knowledge of and expertise in regulatory and commercial issues. Ohad provides local and multinational corporate clients with comprehensive and ongoing legal advice necessary for conducting business in Israel, mainly in the areas of privacy and data protection, consumer protection, e-commerce, food and beverages law, automotive and aviation laws, import, distribution, and agency and corporate governance.
1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?
Since 25 May 2018, the main data protection legislation in the EU is Regulation (EU) No. 2016/679 (the “General Data Protection Regulation” or the “GDPR”). The GDPR repealed Directive 1995/46/EC (the “Data Protection Directive”) and leads to increased harmonisation of data protection law across the EU Member States.

1.2 Is there any other general legislation that impacts data protection?
The main Italian legislation for the protection of personal data is Legislative Decree 196/2003 (hereinafter the “Privacy Code”), recently amended by Legislative Decree 101/2018 in order to adapt it to the changes introduced by the GDPR.

1.3 Is there any sector-specific legislation that impacts data protection?
The following is a non-exhaustive list of the Italian legislation providing for specific rules that impact on data protection:

- L.D. 65/2018 implementing Directive 1148/2016 concerning measures for a high common level of security of network and information systems across the EU;
- L.D. 179/2017 on whistleblowing;
- L.D. 300/1970 (the s.c. “Statute of Workers”);
- L.D. 81/2008 on health and safety at work;
- L.D. 206/2005 (the s.c. “Consumers Code”); and

The Italian Data Protection Authority regularly issues decisions on specific sectors and data protection issues and, pursuant to Article 22, paragraph 4 of L.D. 101/2018, they will continue to apply as long as they comply with the GDPR and the Privacy Code.

1.4 What authority(ies) are responsible for data protection?
The Italian Authority responsible for monitoring the application of the data protection legislation in force is the “Garante per la protezione dei dati personali” (hereinafter referred to as the “Italian DPA”). For the performance of its duties, the Italian DPA, where necessary, may avail itself of the collaboration of other Italian authorities or law enforcement agencies (e.g. the “Guardia di Finanza – Nucleo speciale privacy” for inspection activities).

2 Definitions

2.1 Please provide the key definitions used in the relevant legislation:

- “Personal Data”
Any information relating to a natural person, who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

- “Processing”
Any operation or set of operations which is performed on personal data or sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

- “Controller”
The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

- “Processor”
The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data on behalf of the controller.

- “Data Subject”
An individual who is the subject of the relevant personal data.

- “Sensitive Personal Data”
Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, data concerning health or sex life and sexual orientation, genetic data or biometric data (now defined by the GDPR as “Special categories of personal data”).

- “Data Breach”
A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.
Do the data protection laws apply to businesses established outside the EU if they (either as controllers or processors) process personal data of data subjects who are in the EU in relation to: (i) the offering of goods or services to such data subjects; or (ii) the monitoring of their behaviour so far as it takes place within the EU.

The GDPR applies to:
a) businesses that are established in any EU Member State, and process personal data, either as a controller or processor, and regardless of whether or not the processing takes place in the EU;
b) the processing of personal data by a controller that is not established in any EU Member State, but in a place where Member State law applies by virtue of public international law; and
c) businesses established outside the EU if they (either as controllers or processors) process personal data of data subjects who are in the EU in relation to: (i) the offering of goods or services to such data subjects; or (ii) the monitoring of their behaviour so far as it takes place within the EU.

What are the key principles that apply to the processing of personal data?

Transparency
Personal data must be processed in a transparent manner. Controllers must provide in a concise, transparent, intelligible and easily accessible form, using clear and plain language, certain minimum information to data subjects regarding the processing of their personal data.

Lawful basis for processing
The GDPR provides for an exhaustive list of legal basis making the data processing lawful, of which the following are the most relevant for businesses: (i) prior, freely given, specific, informed and unambiguous consent of the data subject; (ii) the processing is necessary for the performance of a contract to which the data subject is a party, or for the purposes of pre-contractual measures taken at the data subject’s request; (iii) the controller has a legal obligation, under the EU or any EU Member State laws, to perform the relevant processing; or (iv) the processing is necessary for the purposes of legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests, fundamental rights or freedoms of the affected data subjects.

Pursuant to Article 9 of the GDPR, the processing of Special categories of personal data is only permitted under certain conditions, of which the most relevant for businesses are: (i) explicit consent of the data subject; (ii) the processing is necessary in the context of employment law; or (iii) the processing is necessary for the establishment, exercise or defence of legal claims.

Purpose limitation
Personal data may only be collected for specified, explicit and legitimate purposes and must not be further processed in a manner that is incompatible with those purposes.

Data minimisation
Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes of the processing.

Proportionality
See answer above under “Data minimisation”.

Accuracy
Personal data must be accurate and, where necessary, kept up to date. Businesses shall take every reasonable step to ensure that inaccurate personal data are either erased or rectified without delay.

Retention
Personal data must be kept in a form that allows identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

Accountability
The controller shall be responsible for, and be able to demonstrate compliance with, the GDPR and the applicable data protection law. Businesses shall consider data protection and privacy concerns upfront in any process and operation, also by implementing appropriate technical and organisational measures.

Other key principles – please specify

Data protection by design
The controller shall, both at the time of the determination of means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing.

Data protection by default
The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only the relevant personal data are processed.

Individual Rights

What are the key rights that individuals have in relation to the processing of their personal data?

Right of access to data/copies of data
A data subject has the right to obtain from a controller the following information: (i) confirmation of whether, and where, the controller is processing the data subject’s personal data; (ii) information about the purposes of the processing; (iii) the categories of data being processed; (iv) the categories of recipients of personal data; (v) the retention period (or the criteria used to determine that period); (vi) the existence of the other rights provided for by the GDPR; (vii) where the personal data were not collected directly from the data subject, the source of such data; and (viii) the existence of, and an explanation of the logic involved in, as well as the envisaged consequences of, any automated decision-making (including profiling) that has a significant effect on the data subject. Additionally, the data subject may request a copy of the personal data being processed.

Right to rectification of errors
Controllers must ensure that inaccurate or incomplete data are erased or rectified without undue delay.

Right to deletion/right to be forgotten
Data subjects have the right to erasure of their personal data if: (i) the data are no longer needed for the original purpose of
processing (and there is not another lawful purpose to process them); (ii) the data subject withdraws consent, and no other lawful ground exists; (iii) the data subject exercises the right to object, and the controller has no overriding grounds for continuing the processing; (iv) the data have been unlawfully processed; or (v) erasure is necessary for compliance with EU or Italian law.

- **Right to object to processing**
  Data subjects have the right to object, on grounds relating to their particular situation, to the processing of personal data where the processing is either necessary for the performance of a task carried out in the public interest or in the exercise of an official authority vested in the controller, or for the purposes of the legitimate interest of the controller or of a third party.

- **Right to restrict processing**
  Data subjects have the right to restrict the processing of personal data, and the controller may hold and use them for limited purposes, if one of the following applies: (i) the accuracy of the data is contested (only for a period enabling the controller to verify that accuracy); (ii) the processing is unlawful; (iii) the controller no longer needs the data for the original purpose of their processing, but the data subject needs to establish, exercise or defend legal rights; or (iv) verification of overriding grounds is pending, following a request to object to processing.

- **Right to data portability**
  Data subjects have the right to receive from the controller a copy of their personal data in a commonly used machine-readable format, and transmit their personal data from this controller to another or have the data transmitted directly between controllers.

- **Right to withdraw consent**
  Data subjects have the right to withdraw their consent at any time, without affecting the lawfulness of processing made before such withdrawal.

- **Right to object to marketing**
  Data subjects have the right to object to the processing of personal data for direct marketing, including profiling.

- **Right to complain to the relevant data protection authority(ies)**
  Data subjects have the right to lodge complaints with the Italian DPA, if the data subjects live in Italy or the alleged infringement occurred in the Italian jurisdiction.

- **Other key rights – please specify**
  Not applicable.

### 6 Registration Formalities and Prior Approval

#### 6.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?

The obligation of prior notification to the Italian DPA, as provided for the processing of “sensitive data” by Article 37 of the former Privacy Code, has been definitely repealed by Article 22, paragraph 8 of L.D. 101/2018.

Only in one case, pursuant to Article 110-bis of the Privacy Code (as amended by L.D. 101/2018), third parties willing to reuse personal data for scientific research or statistical purposes must notify the Italian DPA whether, due to particular reasons, the obligation to inform the data subjects is impossible, involves a disproportionate effort, or risks seriously compromising the achievement of such research purposes.

Furthermore, under the GDPR, even if it is not a prior notification, the controller should consult the supervisory authority prior to processing where, as a result of a data protection impact assessment (the “DPIA”), that processing would involve a high risk unless the controller implements appropriate measures to mitigate such risk.

#### 6.2 If such registration/notification is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?

This is not applicable (please see question 6.1 above).

#### 6.3 On what basis are registrations/notifications made (e.g., per legal entity, per processing purpose, per data category, per system or database)?

This is not applicable (please see question 6.1 above).

#### 6.4 Who must register with/notify the data protection authority (e.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation)?

This is not applicable (please see question 6.1 above).

#### 6.5 What information must be included in the registration/notification (e.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes)?

This is not applicable (please see question 6.1 above).

#### 6.6 What are the sanctions for failure to register/notify where required?

This is not applicable (please see question 6.1 above).

#### 6.7 What is the fee per registration/notification (if applicable)?

This is not applicable (please see question 6.1 above).

#### 6.8 How frequently must registrations/notifications be renewed (if applicable)?

This is not applicable (please see question 6.1 above).

#### 6.9 Is any prior approval required from the data protection regulator?

This is not applicable (please see question 6.1 above).
6.10 Can the registration/notification be completed online?

This is not applicable (please see question 6.1 above).

6.11 Is there a publicly available list of completed registrations/notifications?

The processing register for notifications required under the former Privacy Code is still publicly accessible; however, it has not been updated since 25 May 2018.

6.12 How long does a typical registration/notification process take?

This is not applicable (please see question 6.1 above).

7 Appointment of a Data Protection Officer

7.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.

The appointment of a Data Protection Officer (hereinafter the “DPO”) is only mandatory when businesses’ core activities consist of data processing which requires: (i) large-scale regular and systematic monitoring of individuals; or (ii) large-scale processing of special categories of personal data.

7.2 What are the sanctions for failing to appoint a Data Protection Officer where required?

Failure to appoint a DPO may result in administrative fines up to €10 million or 2% of worldwide turnover.

7.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect of his or her role as a Data Protection Officer?

When businesses have appointed a staff member or employee as a DPO, he/she shall not be dismissed or penalised for performing his/her tasks.

7.4 Can a business appoint a single Data Protection Officer to cover multiple entities?

A group of undertakings may appoint a single DPO provided that the DPO is easily accessible from each establishment.

7.5 Please describe any specific qualifications for the Data Protection Officer required by law.

The DPO should be appointed on the basis of his/her professional qualities and he/she should have an expert knowledge of data protection laws and practices – which depend on the data processing operations carried out and the protection required for the processed personal data.

7.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?

The DPO shall be involved in all issues relating to the protection of personal data. The DPO shall, at least: (i) inform the controller, processor and their relevant employees of their obligations under the applicable data protection laws; (ii) monitor compliance with applicable data protection laws and internal policies concerning the protection of personal data; (iii) advise on and monitor the performance of a DPIA; and (iv) co-operate with the relevant supervisory authorities and act as a contact point for the latter and the data subjects on issues related to data processing.

7.7 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?

Businesses must notify the contact details of the designated DPO to all the relevant supervisory authorities.

7.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?

While the DPO does not necessarily have to be named in a privacy notice, the latter should include the contact details of the DPO. As a matter of good practice, businesses may also inform their employees of the DPO’s name.

8 Appointment of Processors

8.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?

A business appointing a processor to process personal data on its behalf is required to enter into an agreement with such processor, which sets out the subject-matter, the duration, the nature and purpose of processing, the type of personal data and the categories of data subjects, as well as the obligations and rights of the controller and the processor.

8.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?

The agreement shall be in writing, executed by both parties, and it must stipulate that the processor: (i) only acts on the documented instructions of the controller; (ii) commits itself to confidentiality obligations; (iii) ensures the security of the processed data; (iv) abides by the rules regarding the appointment of sub-processors; (v) implements measures to assist the controller in ensuring the rights of data subjects; (vi) assists the controller in ensuring compliance with the GDPR; (vii) either returns or destroys the personal data at the end of agreement (except as required by EU or Member State law); and (viii) provides the controller with all information necessary to demonstrate compliance with the GDPR.
9 Marketing

9.1 Please describe any legislative restrictions on the sending of electronic direct marketing (e.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?).

The legitimate interests of the controller, including those of a controller to which the personal data may be disclosed, or of a third party, may provide a legal basis for processing for direct marketing purposes, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding.

However, in the case that the controller uses automated call or call communication systems without the intervention of an operator for advertising or commercial purposes, or to do market research, the recipient must have given her/his prior and express consent. This requirement applies also to processing by means of e-mail, fax, MMS or SMS or others.

The controller shall not request the prior consent of the data subject in order to send communications to promote the sale of its products or services, provided that: (i) the data subject previously purchased similar products or services from such controller; (ii) the communications regard services similar to those purchased; and (iii) the data subject is informed and does not object to such use of his/her data.

9.2 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.).

The processing of personal data for marketing purposes through phone calls and mail is permitted towards users who have not exercised the right to object, by registering their number and address in the s.c. “Do Not Call” register.

It follows that each controller monthly or, in any case, prior to any advertising campaign, must verify that the user is not listed in the Do Not Call register and update its databases. If he/she is listed, the operator may refrain from carrying out processing for marketing purposes.

Once a user has subscribed to the “Do Not Call” register:

- the consent given prior to the subscription is annulled and all data controllers to which her/his telephone numbers are communicated are prevented from using them for marketing purposes; and
- the communication to third parties, the transfer and the spread of her/his personal data for advertising, sale and commercial purposes not related to the business (products and services) offered by the data controller, are forbidden.

By contrast, consent given after subscription to the register is valid.

There is no pan-European list including all communication channels, therefore a user willing to stop unsolicited ads should register on her/his domestic “Do Not Call” register and also on each EU Member State register.

9.3 Do the restrictions noted above apply to marketing sent from other jurisdictions?

There is no pan-European list including all communication channels, therefore a user wishing to stop unsolicited ads should register on her/his domestic “Do Not Call” register and also on each EU Member State register.

9.4 Is/are the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?

The Italian DPA is active in such enforcement and in case of breaches of marketing restrictions, issues decisions imposing sanctions on data controllers or processor involved in the unlawful processing. Furthermore, the Italian DPA monitors the lawfulness of profiling activities.

9.5 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?

In order to sell marketing lists to third parties, the controller shall provide the data subjects with a privacy statement including the categories of recipients of their personal data, and obtain a separate and specific consent to such communication from the data subject. A business that purchases marketing lists shall provide the data subjects with a privacy statement including, among other elements, the source of their personal data (i.e. the first data controller).

9.6 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?

Any breach of marketing restrictions is subject to sanctions up to €20 million or up to 4% of worldwide turnover. Furthermore, pursuant to Article 167 of the Privacy Code, if personal data were sold for gain to the data controller or others without consent and the data processing harms the data subject, the data controller shall be punished by imprisonment for six months to one year and a half.

10 Cookies

10.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).

According to the Italian DPA binding note on 8 May 2014, upon accessing a website, a “short” privacy statement must be displayed in a clearly visible banner and should refer to an “extended” privacy statement. The banner must specify:

a) if the website uses profiling cookies; and
b) if the website allows “third-party” cookies (i.e. cookies installed by a different website).

By closing the banner, or using the website, users consent to the use of cookies unless they have disabled them.

10.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?

Cookies may be distinguished into three groups: technical cookies; analytics; and profiling/tracking cookies. No prior consent is required for the use of technical cookies.
10.3 To date, has/have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?

The Italian DPA has issued several decisions imposing sanctions in case of breaches in relation to the use of cookies.

10.4 What are the maximum penalties for breaches of applicable cookie restrictions?

Breaches of applicable cookie restrictions may lead to sanctions up to €20 million or up to 4% of worldwide turnover.

11 Restrictions on International Data Transfers

11.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.

Data transfers to other jurisdictions that are not within the European Economic Area may take place – according to a “layered approach” – if the country ensures an adequate level of protection, or the business has implemented one of the required safeguards, or one of particular conditions specified in the GDPR applies.

11.2 Please describe the mechanisms businesses typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).

When transferring personal data to a country not ensuring an adequate level of protection, businesses must guarantee that there are appropriate safeguards, such as, among others, Standard Contractual Clauses drafted by the EU Commission, the Binding Corporate Rules (“BCRs”), or contractual clauses agreed between the data exporter and data importer.

11.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.

The appropriate safeguards referred to under question 11.2 above may be provided for, without requiring any specific authorisation from a supervisory authority, except for the BCRs and the other safeguards provided for under Article 46.3 of the GDPR, which are subject to authorisation by the competent supervisory authority, and the timing required to obtain it depends on the case.

12 Whistle-blower Hotlines

12.1 What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?

The scope of corporate whistle-blower hotlines is not limited to any particular issue. According to the Opinion No. 1/2006 of the WP29, businesses responsible for the whistle-blowing scheme should carefully assess whether it would be appropriate to limit the number of persons entitled to report alleged misconduct, as well as the number of persons who may be reported through the scheme, in particular in the light of the seriousness of the alleged offences reported.

Pursuant to Article 2-undecies, paragraph 1, let. f) of the Privacy Code, data subjects should not exercise the rights provided by Articles 15 to 22 of the GDPR where the exercise could result in a real and concrete prejudice to the confidentiality of the identity of the whistle-blower who reports, according to Law 179/2017 on whistleblowing, the misconduct he/she has become aware of by performing his/her duties.

12.2 Is anonymous reporting prohibited, strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do businesses typically address this issue?

Anonymous reporting is not prohibited; however, it raises problems as regards the essential requirement that personal data should only be collected fairly. As a rule, the WP29 considered that only identified reports should be communicated through whistleblowing schemes in order to satisfy this requirement. Businesses should not encourage anonymous reports.

An individual who intends to report to a whistle-blowing system should be aware that he/she will not suffer due to his/her action. The whistle-blower, at the time of the first contact with the scheme, should be informed that his/her identity will be kept confidential at all the stages of the process, and will not be disclosed to third parties, such as the incriminated person or to the employee’s line management. Whistle-blowers should be informed that their identity would be disclosed to the relevant people involved in any further investigation or subsequent judicial proceedings instigated as a result of any enquiry conducted by the whistle-blowing scheme.

13 CCTV

13.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?

A DPIA must be undertaken when there is a systematic monitoring of a publicly accessible area on a large scale, such as by using CCTV cameras. If the DPIA suggests that the processing would result in a high risk to the rights and freedoms of individuals prior to any action being taken by the controller, the controller must consult the supervisory authority.

The data subjects must always be informed when they enter a monitored area. The controller can make a “simplified” privacy
statement easily available without charge for the data subjects, indicating who is the controller and the purposes pursued, and referring to an “extended” privacy statement containing all the elements provided for by Article 13 of the GDPR.

13.2 Are there limits on the purposes for which CCTV data may be used?

The Italian DPA has issued various decisions concerning CCTV and their limits (the most relevant is the decision issued on 8 April 2010). Among the most relevant: (i) the controller may use CCTV for the purposes of protection and safety of individuals and property, provided that this does not result in an unjustified interference with the fundamental rights and freedoms of the data subjects; (ii) the installation of a CCTV system must comply not only with the legislation on personal data protection, but also with the other national applicable laws (e.g., those regulating the use of remotely controlled devices for employee monitoring).

The other limits on the use of CCTV do not differ from those provided for by the GDPR which are applicable to the processing of personal data through other means.

14 Employee Monitoring

14.1 What types of employee monitoring are permitted (if any), and in what circumstances?

Employee monitoring shall always be respectful of their fundamental rights, not only with regard to privacy, but also to personal dignity and to freedom of communication and expression. The so-called “Jobs Act” amended Article 4 of the Statute of Workers and it provides for a distinction between CCTV (and remotely controlled devices) and other kinds of monitoring.

The former is allowed only if: i) its use is linked to the organisation or production-related needs, or to the safety of the company’s assets; and ii) there is a trade union agreement or an authorisation by the local labour authority.

The restrictions under points i) and ii) are not applicable to other tools used by the employees directly to perform their tasks (including smartphones, PCs, etc.) or to the apparatus to record access and presence at the workplace. The data controller must not constantly monitor its employees through these tools for work-related purposes either (which include disciplinary purposes).

14.2 Is consent or notice required? Describe how employers typically obtain consent or provide notice.

Employees must be provided with a proper privacy statement concerning all types of processing, including monitoring carried out as above-described. This shall include: information on the existence, manner, compulsory or non-compulsory nature of the processing; the persons or entities which could process such data; the responsible data processors; and the employees’ rights. In the absence of such information to employees, the data cannot be processed.

14.3 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?

Trade unions, namely the internal trade union representatives or, in case of undertakings having their seats in different regions, the most representative national trade union associations need to give their agreement for CCTV (and remotely controlled devices). Where there is no agreement, specific authorisation by the local labour authority is required (see question 14.1 above).

15 Data Security and Data Breach

15.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?

Personal data must be processed in a way which ensures security and safeguards against unauthorised or unlawful processing, accidental loss, destruction and damage of the data.

Both controllers and processors must ensure that they have implemented appropriate technical and organisational measures, which may include: the encryption of personal data; the ability to ensure the ongoing confidentiality, integrity and resilience of processing systems; the ability to restore access to data following a technical or physical incident; and a process for regularly testing and evaluating the technical and organisational measures for ensuring the security of processing.

15.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

The controller is responsible for reporting a data breach without undue delay (and in any case, within 72 hours of first becoming aware of the breach) to the relevant supervisory authority, unless the breach is unlikely to result in a risk to the rights and freedoms of the data subject(s). A processor must notify any data breach to the controller without undue delay.

The notification must include the nature of the personal data breach, including: the categories and number of data subjects concerned; the name and contact details of the DPO or other relevant point of contact; and the likely consequences of the breach and the measures taken to address the breach, including attempts to mitigate possible adverse effects.

15.3 Is there a legal requirement to report data breaches to affected data subjects? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

Controllers have a legal requirement to communicate the breach to the data subjects, without undue delay, if the breach is likely to result in a high risk to the rights and freedoms of the data subject.

The notification must include: the name and contact details of the DPO (or other relevant point of contact); the likely consequences of the breach; and any measures taken to remedy or mitigate the breach. The controller is exempt from communicating the breach to the data subject if the risk of harm is remote, it has taken measures to minimise the risk of harm, or the notification requires a disproportionate effort.
**15.4 What are the maximum penalties for data security breaches?**

Up to €20 million or 4% of worldwide turnover.

**16 Enforcement and Sanctions**

**16.1 Describe the enforcement powers of the data protection authority(ies).**

<table>
<thead>
<tr>
<th>Investigative Power</th>
<th>Civil/Administrative Sanction</th>
<th>Criminal Sanction</th>
</tr>
</thead>
<tbody>
<tr>
<td>Investigative powers</td>
<td>The data protection authority may: order the controller and the processor to provide any information it requires for the performance of its tasks; conduct investigations in the form of data protection audits; carry out review of certificates issued pursuant to the GDPR; notify the controller or processor of alleged infringements of the GDPR; access all personal data and information necessary for the performance of controllers’ or processors’ tasks; and access the premises where the data are kept, including any data processing equipment.</td>
<td>Not applicable.</td>
</tr>
<tr>
<td>Corrective Powers</td>
<td>The data protection authority may: issue warnings or reprimands for non-compliance; order the controller to disclose a personal data breach to the data subject; impose a permanent or temporary ban on processing; withdraw a certification; or impose an administrative fine (as below).</td>
<td>Not applicable.</td>
</tr>
<tr>
<td>Authorisation and Advisory Powers</td>
<td>The data protection authority may: advise the controller; or authorise certificates, contractual clauses, administrative arrangements and binding corporate rules, as outlined in the GDPR.</td>
<td>Not applicable.</td>
</tr>
<tr>
<td>Imposition of administrative fines for infringements of specified GDPR provisions</td>
<td>The GDPR provides for administrative fines, which can be up to €20 million or up to 4% of the business’ worldwide annual turnover of the preceding financial year.</td>
<td>Not applicable.</td>
</tr>
<tr>
<td>Non-compliance with a data protection authority</td>
<td>The GDPR provides for administrative fines which will be up to €20 million or up to 4% of the business’ worldwide annual turnover of the preceding financial year, whichever is higher.</td>
<td>Not applicable.</td>
</tr>
</tbody>
</table>

**16.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?**

The data protection authority has the power to issue a ban on a particular processing activity. The GDPR entitles the relevant supervisory authority to impose a temporary or definitive limitation, including a ban on processing.

**16.3 Describe the data protection authority’s approach to exercising those powers, with examples of recent cases.**

The Italian DPA regularly issues sanctions or bans on particular data-processing activities when due to their nature, methods or effects, these result in significant prejudice to the data subject. For example, the Italian DPA found the processing carried out by a leading tech company to be unlawful because it was grounded on a general consent provided by users upon signing into the platform on the basis of inadequate information. As a consequence, the Italian DPA banned the company from this processing.

**16.4 Does the data protection authority ever exercise its powers against businesses established in other jurisdictions? If so, how is this enforced?**

A data protection authority cannot impose sanctions against a controller established outside its jurisdiction, but can only investigate its activities in the territory of that Member State with the cooperation of the host supervisory authority. In accordance with this principle, the Italian DPA would need to contact the local supervisory authority which is competent in order to seek its cooperation pursuant to Articles 60 to 63 of the GDPR.

**17 E-discovery / Disclosure to Foreign Law Enforcement Agencies**

**17.1 How do businesses typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?**

It actually depends on the legal standing (or entitlement) of the law enforcement agencies to request the e-discovery/disclosure of documents, on the type of documents requested, and on the reasons for requesting. In general, it should be taken into account that, other than privacy limitations, strict attorney-privilege limitations also apply in Italy. It should also be noted that e-discovery and disclosure requests are not part of the Italian legal system.

**17.2 What guidance has/have the data protection authority(ies) issued?**

The Italian DPA has not issued any specific guidance on this topic.

**18 Trends and Developments**

**18.1 What enforcement trends have emerged during the previous 12 months? Describe any relevant case law.**

The Italian DPA has focused its investigations on data processing in the following sectors: i) data processing carried out by companies and public administrations that manage large databases; ii) data protection measures in credit institutions (especially with reference to data breach reports); and iii) data processing for telemarketing activities. In particular, the Italian DPA has investigated and sanctioned several telecommunications companies for aggressive telemarketing and non-compliance with data protection rules.
18.2 What “hot topics” are currently a focus for the data protection regulator?

The Italian DPA has been issuing decisions to fully implement provisions of the Privacy Code. For example, the Italian DPA has reviewed its general authorisations issued in the past, indicating those that are still valid under the GDPR. Furthermore, it recently issued a list of the kind of processing operations subject to a DPIA pursuant to Article 35 paragraph 4 of the GDPR. Further measures are expected in the following months, such as simplified modalities of compliance with the GDPR for small and medium-sized enterprises.

Carlo Impalà
Morri Rossetti e Associati
Studio Legale e Tributario
Piazza E. Duse no. 2
20122 Milan
Italy
Tel: +39 02 760 7971
Email: carlo.impala@morrirossetti.it
URL: www.morrirossetti.it

As Head of the TMT and Data Protection department, Avv. Carlo Impalà provides legal advice to national and international clients. He deals with corporate and commercial law, and the preparation and implementation of corporate governance and compliance models. He has extensive knowledge of the legislation applicable to the internet, online advertising, data protection, TMT, e-commerce, information technology and outsourcing.

Having graduated in Law, magna cum laude, at the University of Palermo, he received an LLM in European Legal Studies at the College of Europe in Bruges (Belgium); he also attended a Masters in the field of Digital Business at the Business School of IlSole24Ore.

Carlo has gained a wide range of professional experience at leading international law firms, both in Italy and abroad, and at the Italian Permanent Representation to the EU in Brussels (Belgium).

Carlo is DPO-certified by KHC, and a member of the IAPP (International Association of Privacy Professionals), Federprivacy, Assofintech, and of AmCham’s GDPR working group.

He has also been included in the “IP&TMT awards ranking 2019” of the legal directories Toplegal and Legalcommunity, among the best lawyers in the media and privacy sectors.

Morri Rossetti offers legal and tax advice to national and international clients operating mainly in the telecommunications, media and technology (TMT) sectors, as well as in the digital innovation, e-commerce and online advertising industries.

The TMT and Data Protection department of Morri Rossetti is composed of professionals specialised in several areas of law (in particular, Corporate and Commercial Law, IT and TMT law, Media Law, Privacy and Data Protection, Cybersecurity, Tax Advisory and Tax Compliance) who are able to offer highly innovative and tailor-made solutions, together with a strong sensitivity and ability to understand the business models of such sectors, the opportunities, as well as the legal and tax-critical features of technological evolution.

The integrated and multidisciplinary advice provided by the TMT Team stands out for its high flexibility and efficiency in terms of fees, with an innovative payment system for the services offered – especially to start-ups.

The TMT and Data Protection department has also received important acknowledgments from leading national and international legal directories (e.g. The Legal 500, Toplegal and Legalcommunity) that have recognised the high profile of the assistance and services provided by the Firm to its clients.
1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

The following laws and regulations have been the basic legislation in Japan for the protection of Personal Information since 2005:

(i) Act on the Protection of Personal Information (Act No. 57 of May 30, 2003, as amended; the “APPI”);
(ii) Act on the Protection of Personal Information Held by Administrative Organs (Act No. 95 of 1988 of May 30, 2003 as amended);
(iii) Act on the Protection of Personal Information Held by Independent Administrative Agencies; and
(iv) local regulations (jyourei) legislated by local governments.

In addition, each Ministry regulating specific industrial sectors issues data protection guidelines for those sectors. Please see question 1.3.

APPI

The APPI is the principal data protection legislation. It is the APPI’s basic principle that the cautious handling of Personal Information, as defined in Article 2, paragraph 1, under the principle of respect for individuals, will promote the proper handling of Personal Information (APPI, Article 3).

Chapters 2 and 3 set forth the basic frameworks of the responsibilities and policies of the national and local governments to protect Personal Information. Pursuant to Article 7 of the APPI, the Cabinet established the “Basic Policy on the Protection of Personal Information” (Kojin Jyouhou no Hogo ni kansuru Kihon Houshin) in 2004 (as amended; the “Basic Policy”).

Chapter 4 regulates the use of Personal Information by private businesses and sets forth the obligations of “Business Operators Handling Personal Information (Kojin Joho Toriatsukai Jigyosha)” (the “Handling Operators”), as defined in Article 2, paragraph 5 of the APPI. Before the amendment of the APPI, Handling Operators included all business operators using a Personal Information Database for their businesses (please see question 2.1), except for business operators with fewer than 5,000 individuals in their Personal Information Database at any time in the past six months. This exception will no longer be available upon the full effectivity of the Amended APPI. Note that administrative organs and independent administrative agencies are not Handling Operators and their data handling is regulated under the laws described in items (ii) and (iii) of the laws listed in the first paragraph above.

Privacy Mark

A business operator may use a logo called a “Privacy Mark” (the “Privacy Mark System”) which shows its compliance with the relevant laws and the Japan Industrial Standards (JIS Q 15001:2006 [Personal Information Protection Management System – Requirements]) (“JIS Q 15001”) established by the Japan Information Processing Development Center. JIS Q 15001 is not a law but, in certain aspects, it provides a higher level of standards than the APPI.

On May 30, 2017, amendments to (i) the APPI, (ii) the Act on the Utilisation of Numbers to Identify Specific Individuals in Administrative Procedures (Act No. 27 of 31 May 2013, as amended; the “My Number Act”), and (iii) other relevant laws were brought fully into force. Amendments to the APPI (the “Amended APPI”) include:

- Establishing the Personal Information Protection Committee (the “PPC”), which will supervise the enforcement and application of the APPI.

- Introducing the definition of Sensitive Personal Information.

- Introducing restrictions on transferring Personal Data to foreign jurisdictions.

The PPC was established on January 1, 2016. The Cabinet Order and the ordinance issued by the PPC (the “PPC Ordinance”), which provide for the details of the Amended APPI, were promulgated on October 5, 2016.

APPI

The APPI is the principal data protection legislation. It is the APPI’s basic principle that the cautious handling of Personal Information, as defined in Article 2, paragraph 1, under the principle of respect for individuals, will promote the proper handling of Personal Information (APPI, Article 3).

Chapters 2 and 3 set forth the basic frameworks of the responsibilities and policies of the national and local governments to protect Personal Information. Pursuant to Article 7 of the APPI, the Cabinet established the “Basic Policy on the Protection of Personal Information” (Kojin Jyouhou no Hogo ni kansuru Kihon Houshin) in 2004 (as amended; the “Basic Policy”).

Chapter 4 regulates the use of Personal Information by private businesses and sets forth the obligations of “Business Operators Handling Personal Information (Kojin Joho Toriatsukai Jigyosha)” (the “Handling Operators”), as defined in Article 2, paragraph 5 of the APPI. Before the amendment of the APPI, Handling Operators included all business operators using a Personal Information Database for their businesses (please see question 2.1), except for business operators with fewer than 5,000 individuals in their Personal Information Database at any time in the past six months. This exception will no longer be available upon the full effectivity of the Amended APPI. Note that administrative organs and independent administrative agencies are not Handling Operators and their data handling is regulated under the laws described in items (ii) and (iii) of the laws listed in the first paragraph above.

Privacy Mark

A business operator may use a logo called a “Privacy Mark” (the “Privacy Mark System”) which shows its compliance with the relevant laws and the Japan Industrial Standards (JIS Q 15001:2006 [Personal Information Protection Management System – Requirements]) (“JIS Q 15001”) established by the Japan Information Processing Development Center. JIS Q 15001 is not a law but, in certain aspects, it provides a higher level of standards than the APPI.
1.2 Is there any other general legislation that impacts data protection?

(a) Privacy Right

The privacy right is recognised by Japanese courts as the right of persons for their private life not to be disclosed except for a legitimate reason, and is recognised among academics as the right to control one’s own Personal Information. Therefore, in addition to complying with the APPI, a person who possesses the Personal Information of others in Japan must not infringe on the privacy rights of the principals.

(b) Privacy of Communications

Article 4 of the Telecommunications Business Law provides that no person may infringe on the privacy of the communications handled by telecommunications business operators. Privacy of communications does not necessarily refer to Personal Information, although the guidelines issued by the Ministry of Internal Affairs and Communications (“MIAC”) for the protection of Personal Information in the telecommunication business (please see question 1.3) also deal with the privacy of communications, such as telecommunications logs (the “MIAC Guidelines”).

(c) Electronic Mails


(d) Commercial Transactions

The Act on Specified Commercial Transactions (Act No. 57 of June 4, 1976, as amended) regulates, among other forms of unsolicited marketing, unsolicited marketing by email. Please see question 9.1.

(e) Utilisation of Numbers to Identify Individuals in Administrative Procedures

The Japanese government adopted a social security and tax number system and in 2015 assigned specific numbers to entities and individuals pursuant to the My Number Act. It is the basic principle of this law that using the assigned numbers will contribute to the efficient and prompt exchange of information by administrative organs. Under this law, the assigned numbers should be handled duly and safely in accordance with certain standards, which are different from those under the APPI and the laws described in items (ii) and (iii) of the laws listed in the first paragraph of the answer to question 1.1.

1.3 Is there any sector-specific legislation that impacts data protection?

There was no single independent regulatory authority that was responsible for implementing the previous APPI. Each Ministry that regulates specific industries was responsible for enforcing the previous APPI in that industry. In this regard, each Ministry regulating specific industries issued guidelines for those industries. The Amended APPI established the PPC, which is responsible overall for implementing the APPI. The PPC issues guidelines on the principles of the APPI. However, in some industries, there remain specific guidelines which were issued by other ministries, such as (i) telecommunications guidelines issued by MIAC, (ii) broadcasting guidelines issued by MIAC, (iii) posting guidelines issued by MIAC, and (iv) genetic information guidelines issued by the Ministry of Economy, Trade and Industry. Further, the PPC and the Ministry of Finance have jointly issued certain financial affairs guidelines, while the PPC and the Ministry of Health, Labour and Welfare have jointly issued certain medical care guidelines.

1.4 What authority(ies) are responsible for data protection?

Under the previous APPI, the Minister of each Ministry regulating a specific industry was responsible for the supervision and enforcement of the APPI in that industry. Under the Amended APPI, however, the PPC, as an independent regulatory body, is authorised to advise a Handling Operator or require it to prepare and submit a report on the handling of Personal Information to the extent necessary to implement the APPI (APPI, Articles 40 and 41). If a Handling Operator violates the APPI, the PPC may urge it to cease the violation and take other necessary measures to correct the violation (Id. Article 42, paragraph 1). If the PPC finds it necessary and certain requirements are met, it may order the Handling Operator to take the urged measures or to cease the violation and take other necessary measures to rectify the violation (Id. Article 42, paragraphs 2 and 3). The PPC is also responsible for the supervision and enforcement of the My Number Act (My Number Act, Article 33).

Please also see question 1.1.

2 Definitions

2.1 Please provide the key definitions used in the relevant legislation:

“Personal Data”

The APPI provides for four definitions relevant to Personal Data:

“Personal Information” is information about living individuals which (a) can identify specific individuals, or (b) contains an “Individual Identification Code”. Information which can identify specific individuals under clause (a) of the definition includes information which can be readily collated with other information to identify specific individuals.

The “Individual Identification Code” under clause (b) of the definition is a new concept introduced by the APPI Amendments (APPI, Article 2, paragraph 1). This refers to any character, number, symbol or other code (i) into which a partial body feature of a specific individual has been converted by computers for use and which can identify such specific individual, or (ii) which is assigned to services or goods provided to an individual, or is stated or electromagnetically recorded on a card or other documents issued to an individual (such as a driver’s licence number), to identify him/her as a specific user, purchaser, or recipient of the issued document (APPI, Article 2, paragraph 2).

“Personal Information Database” means an assembly of information including the following: (i) an assembly of information systematically arranged in such a way that specific Personal Information can be retrieved by a computer; and (ii) an assembly of information designated by a Cabinet Order as being systematically arranged in such a way that specific Personal Information can be easily retrieved. However, any assembly of information the use of which is not likely to harm the interests of the individual principals, as further set out in the Cabinet Order of the APPI, is excluded from the definition (Id. Article 2, paragraph 4).

“Personal Data” means Personal Information constituting a Personal Information Database (Id. Article 2, paragraph 6).

“Retained Personal Data” means Personal Data which a Handling Operator has the authority to disclose, correct, add, erase or delete, discontinue its utilisation, or discontinue its provision to a third party, excluding the following (Id. Article 2, paragraph 7).
What are the key principles that apply to the processing of Personal Data?

3 Territorial Scope

3.1 Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to those laws?

The APPI in force prior to the APPI Amendments did not explicitly provide for its application outside Japan. After the APPI Amendments, however, key provisions of the APPI apply to entities outside Japan if they receive Personal Information in connection with the provision of goods or services to individuals residing in Japan (APPI, Article 75).

4 Key Principles

4.1 What are the key principles that apply to the processing of personal data?

- **Purpose limitation**
  Handling Operators are required to specify the purposes of utilisation of Personal Information to the extent possible and not to use the Personal Information of any person, without obtaining the consent of that person, beyond the scope necessary to achieve the specified purpose of utilisation of Personal Information (Id. Articles 15 and 16). Further, Handling Operators are required to endeavour to keep Personal Information accurate and up to date within the scope necessary to achieve the purpose of utilisation of Personal Information (Id. Article 19).

- **Data minimisation**
  The APPI imposes no obligation to minimise the Personal Information which Handling Operators may obtain or use.

Other key definitions – please specify (e.g., “Pseudonymous Data”, “Direct Personal Data”, “Indirect Personal Data”)

- **“Anonymously Processed Information”**, which was not defined in the APPI prior to its amendment, is defined in the Amended APPI as information obtained by processing Personal Information such that ordinary people cannot (a) identify a specific principal using the processed information, or (b) restore any Personal Information from the processed information (APPI, Article 2.9).

- **“Lawful basis for processing”**
  The APPI has no provision explicitly dealing with transparency. However, Handling Operators are required to either publicly announce or notify the principals of the purposes of utilisation of their Personal Information promptly after the collection of Personal Information (subject to certain exceptions) (APPI, Article 18).

Further, the Basic Policy requires Handling Operators to establish and publicly disclose their privacy policy or privacy statement, as well as their use of service providers to handle collected Personal Information and the extent of the service.

- **“Data Breach”**
  “Data Breach” is not a term under the APPI; however, regarding Personal Data, the PPC’s Notification No. 1 (2017) defines a breach of data security as a leakage of, loss of, or damage to data.

- **“Sensitive Personal Data”**
  “Sensitive Personal Data”, which was not defined in the APPI prior to its amendment, is defined in the Amended APPI as information obtained by processing Personal Information such as not to cause social discrimination, prejudice or other disadvantages (APPI, Article 2, paragraph 8). The Cabinet Order for the Amended APPI provides details of what constitutes Sensitive Personal Data, which include physical or mental disabilities, results of medical examinations conducted by doctors or personnel who are engaged in medical services, records of medical treatment or medical advice provided based on the results of medical examinations or due to a disease, an injury or other changes in physical or mental conditions, and history related to criminal procedures such as arrest, investigation or detention.

- **“Lawful basis for processing”**
  Handling Operators are prohibited from acquiring Personal Information by deception or other wrongful means (Id. Article 17). They are also prohibited from acquiring Sensitive Personal Information without the consent of the principal except:
  (i) if required by laws and regulations;
  (ii) if necessary to protect the life, body, or property of a person and it is difficult to obtain the consent of the principal;
  (iii) if necessary to improve public health and promote the sound nurturing of the young and it is difficult to obtain the consent of the principal;
  (iv) if necessary for governmental bodies to perform their business and getting the consent of the principal will likely impede the proper performance of business; or
  (v) for Sensitive Personal Information that has been disclosed to the public by the principal, governmental bodies, or certain parties designated by the PPC (e.g., foreign governments and international organisations).

- **“Controller”**
  Please see the definition of “Processor” below.

- **“Data Subject”**
  The term “principal” would be comparable to a “Data Subject”. Article 2, paragraph 8 of the APPI defines “principal” as a specific individual identified by Personal Information.

- **“Sensitive Personal Data”**
  “Sensitive Personal Data”, which was not defined in the APPI prior to its amendment, is defined in the Amended APPI as information obtained by processing Personal Information which needs careful handling so as not to cause social discrimination, prejudice or other disadvantages (APPI, Article 2, paragraph 8). The Cabinet Order for the Amended APPI provides details of what constitutes Sensitive Personal Data, which include physical or mental disabilities, results of medical examinations conducted by doctors or personnel who are engaged in medical services, records of medical treatment or medical advice provided based on the results of medical examinations or due to a disease, an injury or other changes in physical or mental conditions, and history related to criminal procedures such as arrest, investigation or detention.

- **“Data Breach”**
  “Data Breach” is not a term under the APPI; however, regarding Personal Data, the PPC’s Notification No. 1 (2017) defines a breach of data security as a leakage of, loss of, or damage to data.

- **“Processor”**
  The APPI does not use “Controller” or “Processor”. However, a Handling Operator (Kojin Joho Toriatsukai Jigyosha) may be comparable to a Controller or a Processor in that it is subject to obligations to protect Personal Information. Please see question 1.1 for the definition of a Handling Operator. Foreign companies doing business in Japan will be regulated as Handling Operators if they fall within the definition.

- **“Data Breach”**
  “Data Breach” is not a term under the APPI; however, regarding Personal Data, the PPC’s Notification No. 1 (2017) defines a breach of data security as a leakage of, loss of, or damage to data.

- **“Controller”**
  Please see the definition of “Processor” below.

- **“Data Subject”**
  The term “principal” would be comparable to a “Data Subject”. Article 2, paragraph 8 of the APPI defines “principal” as a specific individual identified by Personal Information.

- **“Sensitive Personal Data”**
  “Sensitive Personal Data”, which was not defined in the APPI prior to its amendment, is defined in the Amended APPI as information obtained by processing Personal Information which needs careful handling so as not to cause social discrimination, prejudice or other disadvantages (APPI, Article 2, paragraph 8). The Cabinet Order for the Amended APPI provides details of what constitutes Sensitive Personal Data, which include physical or mental disabilities, results of medical examinations conducted by doctors or personnel who are engaged in medical services, records of medical treatment or medical advice provided based on the results of medical examinations or due to a disease, an injury or other changes in physical or mental conditions, and history related to criminal procedures such as arrest, investigation or detention.

- **“Data Breach”**
  “Data Breach” is not a term under the APPI; however, regarding Personal Data, the PPC’s Notification No. 1 (2017) defines a breach of data security as a leakage of, loss of, or damage to data.

- **“Processor”**
  The APPI does not use “Controller” or “Processor”. However, a Handling Operator (Kojin Joho Toriatsukai Jigyosha) may be comparable to a Controller or a Processor in that it is subject to obligations to protect Personal Information. Please see question 1.1 for the definition of a Handling Operator. Foreign companies doing business in Japan will be regulated as Handling Operators if they fall within the definition.

- **“Data Subject”**
  The term “principal” would be comparable to a “Data Subject”. Article 2, paragraph 8 of the APPI defines “principal” as a specific individual identified by Personal Information.

- **“Sensitive Personal Data”**
  “Sensitive Personal Data”, which was not defined in the APPI prior to its amendment, is defined in the Amended APPI as information obtained by processing Personal Information which needs careful handling so as not to cause social discrimination, prejudice or other disadvantages (APPI, Article 2, paragraph 8). The Cabinet Order for the Amended APPI provides details of what constitutes Sensitive Personal Data, which include physical or mental disabilities, results of medical examinations conducted by doctors or personnel who are engaged in medical services, records of medical treatment or medical advice provided based on the results of medical examinations or due to a disease, an injury or other changes in physical or mental conditions, and history related to criminal procedures such as arrest, investigation or detention.
Proportionality
The APPI has no provision on proportionality.

RetentionPolicy
Handling Operators are required to endeavour to delete Personal Information if its utilisation is no longer necessary (Id. Article 19). Further, there may be other restrictions under industry guidelines. For example, the MIAC Guidelines provide that telecommunication business operators must fix the retention period for the purpose of utilisation of Personal Information, and erase Personal Information after the expiration of the retention period without delay (MIAC Guidelines, Article 10).

Other key principles – please specify
Restriction on provision of Personal Data to a third party
A Handling Operator is prohibited from providing Personal Data to a third party without obtaining the prior consent of the principal, subject to certain exceptions (APPI, Article 23, paragraph 1), such as when the Handling Operator: (a) agrees to stop providing the Personal Data to the third party upon the demand of the principal; (b) notifies the principal of the provision to a third party or makes such notification readily accessible to the principal; and (c) submits a notification to the PPC stating (i) that the provision to third parties is included in the purpose of utilisation, (ii) the items to be provided to third parties, (iii) the mode of provision (e.g., by publishing a book or uploading to a website through the Internet), (iv) the availability of opt-out for the principal who may request the Handling Operator to stop the provision, and (v) the mode of receiving the principal’s request (e.g., telephone, email, or any written material) (Id. Article 23, paragraph 2).

Exceptions
The obligations imposed on Handling Operators will not apply to Handling Operators that fall under any of the following items and if all or part of the purpose of handling Personal Information is prescribed in the following applicable items (Id. Article 76):

(i) broadcasting institutions, newspaper publishers, communication agencies and other forms of the press (including individuals engaged in news reporting as their business); for the purpose of news reporting;
(ii) business operators in the business of literary work; for the purpose of literary work;
(iii) colleges, universities, other institutions or organisations engaged in academic studies, or entities belonging to any of the foregoing entities; for the purpose of academic studies;
(iv) religious organisations; for the purpose of religious activities (including activities incidental thereto); or
(v) political organisations; for the purpose of political activities (including activities incidental thereto).

5 Individual Rights

5.1 What are the key rights that individuals have in relation to the processing of their personal data?

Right of access to data/copies of data
A Handling Operator is required to make accessible to the principal certain information (such as the name of the Handling Operator, the purpose of utilisation of Personal Information, and the procedures for notification of such information to the principal, correction of Personal Information or discontinuation of the utilisation of Personal Information) regarding Retained Personal Data (APPI, Article 27, paragraph 1). Further, if a person requests a Handling Operator to notify him or her of the purpose of utilisation of such Retained Personal Data which may lead to the identification of the person concerned, the Handling Operator must meet the request without delay, subject to certain exceptions (Id. Article 27, paragraph 2).

The exceptions are cases where:
(i) the purposes of utilisation are evident from the information made available to the person by the Handling Operators pursuant to Article 27, paragraph 1 of the APPI;
(ii) publicly announcing or notifying the person of the purpose of utilisation is likely to harm the life, body, property, or other rights or interests of that person or a third party;
(iii) publicly announcing or notifying the person of the purpose of utilisation is likely to harm the rights or legitimate interests of the Handling Operator; or
(iv) it is necessary to cooperate with an administrative organ or a local government in implementing laws and regulations, and publicly announcing or notifying the person of the purpose of utilisation is likely to impede that implementation.

In addition, the Handling Operator is required to disclose, without delay, and upon the request of an individual, that person’s Retained Personal Data, subject to certain exceptions (Id. Article 28). The exceptions are cases where:
(i) disclosure will likely harm the life, body, property, or other rights or interests of the person or a third party;
(ii) disclosure will likely seriously impede the proper execution of the business of the Handling Operator; or
(iii) disclosure will violate other laws and regulations.

The Handling Operator may charge a fee for complying with a request to notify the purpose of utilisation pursuant to Article 27 or to disclose Retained Personal Data pursuant to Article 28.

Right to rectification of errors
The principal may request the Handling Operator to correct, add or delete Retained Personal Data if the Retained Personal Data are not correct. The Handling Operator must investigate without delay, and based on the results of the investigation, correct, add or delete, as requested by the principal, the Retained Personal Data to the extent necessary to achieve the purposes of use (Id. Article 29).

Right to deletion/right to be forgotten
As above, the principal may request the Handling Operator to correct, add or delete Retained Personal Data if the Retained Personal Data are not correct. There is no explicit legal provision on the “right to be forgotten”. Please see question 18.2 for the recent discussion regarding the “right to be forgotten”.

Right to object to processing
The principal may request a Handling Operator (a) to discontinue the use of, or erase, the Retained Personal Data, and (b) to stop providing the Retained Personal Data to third parties if such use or disclosure is or was made, or the Retained Personal Data in question was obtained, in violation of the APPI. The Handling Operator must discontinue the use of, or the provisions to third parties of, or erase, Retained Personal Data upon the request of the principal if the request has reasonable grounds (Id. Article 30).

However, this obligation will not apply if it will be too costly or difficult to discontinue the use of, or to erase, the Retained Personal Data and the Handling Operator takes necessary alternative measures to protect the rights and interests of the principal.
Right to restrict processing
There is no “right to restrict processing” which differs from the rights stipulated above in “Right to object to processing”.

Right to data portability
While legal problems regarding data portability have been the subject of recent intensive discussions, no specific laws or regulations regarding data portability exist to date.

Right to withdraw consent
There is no explicit stipulation regarding the right to withdraw consent under the APPI.

Right to object to marketing
There are no provisions explicitly setting forth objections to marketing. Any objection to marketing would be dealt with as an objection to processing.

Right to complain to the relevant data protection authority(ies)
The individuals may complain to the PPC and the PPC will conduct necessary mediation regarding a lodged complaint (Id. Article 61(ii)).

Other key rights – please specify
Complaint to Authorised Entities for Protection of Personal Information (Nintei Kojin Jyouhou Hogo Dantai)
Authorised Entities for the Protection of Personal Information (Nintei Kojin Jyouhou Hogo Dantai) are entities authorised by the PPC to handle complaints from individuals on the handling of personal information by Handling Operators. As of April 2018, 43 entities have obtained such authorisation.

When an Authorised Entity for the Protection of Personal Information is requested by an individual to resolve a complaint about the handling of Personal Information by a Handling Operator, it must promptly notify the Handling Operator of the complaint and give necessary advice, investigate the circumstances pertaining to the complaint and request the Handling Operator to resolve the complaint promptly. It may, if necessary, request the Handling Operator to explain in writing or orally, or request it to submit relevant materials. The Handling Operator may not reject such request without a justifiable ground (Id. Article 52).

6 Registration Formalities and Prior Approval

6.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?

The APPI imposes no requirement on a Handling Operator to register or notify the PPC to process Personal Information. However, if the Handling Operator provides Personal Information to third parties without obtaining the prior consent of the principals, it is required to notify the PPC (please see question 4.1).

The PPC is also authorised to enter offices or other places, to make inquiries and investigate, and to require a Handling Operator to report or submit materials regarding the handling of Personal Information or Anonymously Processed Information, to the extent necessary to implement the APPI (Id. Articles 40 and 41). Please see question 1.4.

6.2 If such registration/notification is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?

Please see question 6.1.

6.3 On what basis are registrations/notifications made (e.g., per legal entity, per processing purpose, per data category, per system or database)?

Please see question 6.1.

6.4 Who must register with/notify the data protection authority (e.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation)?

Please see question 6.1.

6.5 What information must be included in the registration/notification (e.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes)?

Please see question 6.1.

6.6 What are the sanctions for failure to register/notify where required?

Please see question 6.1.

6.7 What is the fee per registration/notification (if applicable)?

Please see question 6.1.

6.8 How frequently must registrations/notifications be renewed (if applicable)?

Please see question 6.1.

6.9 Is any prior approval required from the data protection regulator?

Please see question 6.1.

6.10 Can the registration/notification be completed online?

Please see question 6.1.

6.11 Is there a publicly available list of completed registrations/notifications?

Please see question 6.1.
6.12 How long does a typical registration/notification process take?

Please see question 6.1.

7 Appointment of a Data Protection Officer

7.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.

The APPI has no provision mandating the appointment of a Privacy or Data Protection Officer. However, the Handling Operator is required to take necessary and proper measures for the prevention of leakage, loss, or damage, and for other security control, of Personal Data (APPI, Article 20). Under the PPC Guidelines, those measures should include the following:

(i) organisational security measures, such as establishing rules for handling Personal Data, and specifying the person responsible for supervising the handling of Personal Data;
(ii) human resource security measures, including the education of employees;
(iii) physical security measures, including controlling the area where Personal Data is handled, such as servers and offices; and
(iv) technical security measures, including controlling access to Personal Data.

The PPC Guidelines indicate that appointing a person to be in charge of the handling of Personal Data is an example of a proper and necessary measure.

7.2 What are the sanctions for failing to appoint a Data Protection Officer where required?

Although a Handling Operator is expected to adopt the measures described in the PPC Guidelines, the failure to adopt such measures is not a direct breach of the APPI.

7.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect of his or her role as a Data Protection Officer?

There is no special protection.

7.4 Can a business appoint a single Data Protection Officer to cover multiple entities?

Please see question 7.1.

7.5 Please describe any specific qualifications for the Data Protection Officer required by law.

Please see question 7.1.

7.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?

Please see question 7.1.

7.7 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?

There is no requirement for the appointment of a Data Protection Officer to be registered or notified.

7.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?

There is no requirement for a Data Protection Officer to be named in a public notice.

8 Appointment of Processors

8.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?

There is no concept of “processor” under the APPI (please see question 2.1). However, there is a concept of “entrustment” of the handling of Personal Data, in which entering into an agreement is recommended.

Under Article 23, paragraph 5(i) of the APPI, if the Handling Operator entrusts all or part of the handling of the Personal Data it acquires to an individual or another entity, that individual or entity will not be considered a “third party” under Article 23, paragraph 1. For example, if the Handling Operator uses third-party vendors for the services, and it shares Personal Data with those third-party vendors for them to use on the Handling Operator’s behalf, and not for their own use, such transfer will be deemed an “entrustment” and the restrictions on the provision of Personal Data to a third party will not apply.

When the Handling Operator “entrusts” Personal Information, it must exercise the necessary and appropriate supervision over the entrusted person to ensure security control over the entrusted Personal Data. The Handling Operator must ensure that the entrusted person (e.g., the third-party service provider) has taken the same appropriate measures that the Handling Operator is required to take. The PPC Guidelines provide that “necessary and appropriate supervision” includes appropriately selecting the service provider, concluding the necessary contracts so that the security control measures based on Article 20 of the APPI are observed by the service provider, and knowing the status of the handling of the Personal Data that was entrusted to the service provider.

8.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?

PPC Guidelines provide that it is desirable to include the agreed security control measures and a provision that allows the Handling Operator to reasonably understand the status of the handling of Personal Data by the service provider.
## Marketing

### 9.1 Please describe any legislative restrictions on the sending of electronic direct marketing (e.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?).

Unsolicited marketing by email is regulated principally by the Act on the Regulation of the Transmission of Specified Electronic Mail (Act No. 26 of April 17, 2002, as amended; the “Anti-Spam Act”). Pursuant to the Anti-Spam Act, marketing emails can be sent only to recipients (i) who “opted in” to receive them, (ii) who provided the sender with their email address in writing (for instance, by providing a business card), (iii) who have a business relationship with the sender, or (iv) who make their email address available on the internet for business purposes. In addition, the Anti-Spam Act requires the senders to allow the recipients to “opt out”. The Anti-Spam Act on Specified Commercial Transactions also adopts the opt-in system for unsolicited marketing.

### 9.2 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.).

Unsolicited telephone marketing regarding certain items such as financial instruments (e.g., derivatives) is restricted under different regulations. There is no national opt-out register system.

### 9.3 Do the restrictions noted above apply to marketing sent from other jurisdictions?

The Anti-Spam Act will apply to any entity, whether or not it has a presence in Japan, even if its marketing emails are sent from outside Japan, as long as the receiver is in Japan.

### 9.4 Is/are the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?

The MIAC and the Consumer Affairs Agency are the authorities in charge of enforcement of the Anti-Spam Act. There have been several enforcement cases initiated by those authorities, including a recent enforcement in March 2018.

### 9.5 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?

Purchasing a marketing list in itself is not illegal; however, if the list is created or shared in a manner that is in breach of the APPI, (the seller and) the purchaser may be subject to a penalty under the APPI. The maximum penalty is either imprisonment of up to one year or a fine of up to 500,000 yen (APPI, Article 83).

### 9.6 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?

The maximum penalties under the Anti-Spam Act are one year of imprisonment or a fine of 1,000,000 yen for an individual, and a fine of 30,000,000 yen for the legal entity which employed that individual.

## Cookies

### 10.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).

The use of cookies or other similar technology is not directly regulated under the APPI; however, if Personal Data are collected through such technology, such Personal Data is subject to the APPI.

### 10.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?

Please see question 10.1.

### 10.3 To date, has/have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?

Please see question 10.1.

### 10.4 What are the maximum penalties for breaches of applicable cookie restrictions?

Please see question 10.1.

## Restrictions on International Data Transfers

### 11.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.

Before the amendment, the APPI did not restrict the transfer of Personal Data abroad. The Amended APPI, however, imposes restrictions on the overseas transfer of Personal Information (APPI, Article 24). These restrictions include requiring the prior consent of the principals to the transfer of their Personal Information to a third party located in a foreign country. However, the principals’ prior consent to overseas data transfers of their Personal Information is not necessary if (i) the foreign country is specified in the PPC Ordinance as having a data protection regime with a level of protection equivalent to that of Japan, or (ii) the third-party recipient has a system of data protection which meets the standards to be prescribed by the PPC Ordinance.

As of January 23, 2019, the PPC has specified the EU as foreign countries having a data protection regime with a level of protection equivalent to that of Japan by the PPC Ordinances (item (1) above). As of the same date, the European Commission also adopted the adequacy decision on Japan in accordance with Article 45 of the GDPR.

The PPC issued the Supplementary Rules for the Personal Data, which has been transferred from the EU by the adequacy decision. By the Supplementary Rules, the handling operators are subject to stricter regulations with regard to Personal Data, which have been transferred from the EU by the adequacy decision.

The PPC Ordinance also provides that with respect to item (ii), the third-party foreign recipient must either (a) provide assurance by appropriate and reasonable methodologies that it will treat the transferred Personal Information pursuant to the spirit of the requirements for the handling of Personal Information under the APPI, or (b) have been certified under a PPC-recognised international...
arrangement regarding its system of handling Personal Information (to date, the only PPC-recognised international arrangement is the APEC Cross-Border Privacy Rules System).

11.2 Please describe the mechanisms businesses typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).

Please see question 11.1.

11.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.

Please see question 11.1.

12 Whistle-blower Hotlines

12.1 What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?

The Whistle-Blower Protection Act (Koueki Tsuhosha Hogo Hou) prohibits employers from dismissing whistle-blowers. The Act itself does not have requirements for companies to have a whistle-blower hotline or system, but the Consumer Affairs Agency has published guidelines for private entities to establish and operate whistle-blower hotlines. The guidelines also specify several measures which companies must implement to protect the Personal Information of whistle-blowers, such as limiting the persons who can access documents regarding the whistle-blowing.

12.2 Is anonymous reporting prohibited, strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do businesses typically address this issue?

Anonymous reporting is generally permitted.

13 CCTV

13.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?

There are no registration/notification requirements for the use of CCTV under the APPI. However, according to the Q&A regarding the PPC Guidelines published by the PPC, it is desirable to take measures so that the individual in question may recognise that his/her Personal Information is being obtained, through visible notices stating that CCTV is in operation. Further, it is desirable to display contact information, a website URL or a QR code in a notice located near CCTV, so that the individual may confirm the relevant information regarding the CCTV.

13.2 Are there limits on the purposes for which CCTV data may be used?

There are no special restrictions for CCTV data which differ from restrictions on other Personal Data under the APPI.

14 Employee Monitoring

14.1 What types of employee monitoring are permitted (if any), and in what circumstances?

The employer has the right to monitor workplace communications in relation to work. However, a privacy issue may arise regarding private communications at the workplace. Thus, it is recommended that employers establish internal rules prohibiting the use of company PCs and email addresses for private use, and disclosing the possibility of monitoring those devices and data.

14.2 Is consent or notice required? Describe how employers typically obtain consent or provide notice.

Please see question 14.3.

14.3 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?

There are no statutory and special requirements for notification to or consultation with trade unions/employee representatives regarding employee monitoring. However, if an employer sets up internal rules on employee monitoring, these rules will be considered company work rules and would require prior notification to or consultation with the majority union or employee representative.

15 Data Security and Data Breach

15.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?

A Handling Operator is obligated to take necessary and proper measures to prevent leakage, loss, or damage, and for other security control, of Personal Data (APPI, Article 20). Further, the Handling Operator is required to exercise necessary and appropriate supervision over its employees and service providers to ensure the security control of Personal Data (Id. Articles 21 and 22). There is no concept of controllers or processors under the APPI (please see question 2.1).

15.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

Under the PPC’s Notification, a Handling Operator must endeavour
to report a breach to the government through the PPC, an Accredited Personal Information Protection Organisation, or any other supervising authority or organisation. However, reporting is not required in the following cases:

(i) the Handling Operator has determined that a Personal Data leakage has not substantially occurred; or
(ii) there have been minor wrong transmissions of email or fax or erroneous dispatch of a package.

Under the financial affairs guidelines (please see question 1.3), a Handling Operator in the financial sector must report any leakage of Personal Information to the Financial Services Agency immediately.

15.3 Is there a legal requirement to report data breaches to affected data subjects? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

The PPC’s Notification provides that it is preferable for a Handling Operator to notify the principal who may be affected by the data breach in order to prevent further damage, and to publicly announce the fact of the data breach and its recurrence prevention measure in order to prevent further damage and similar data breaches in other companies.

15.4 What are the maximum penalties for data security breaches?

If a Handling Operator provides or misuses a Personal Information Database for the purpose of unlawful gains, it may be subject to imprisonment of up to one year, or a fine of up to 500,000 yen (Id. Article 83). If the breach is committed by a person who is employed by an entity, such entity will be subject to the same penalty (Id. Article 87).

16 Enforcement and Sanctions

16.1 Describe the enforcement powers of the data protection authority(ies).

<table>
<thead>
<tr>
<th>Investigatory Power</th>
<th>Civil/Administrative Sanction</th>
<th>Criminal Sanction</th>
</tr>
</thead>
<tbody>
<tr>
<td>Personal Information Protection Committee (&quot;PPC&quot;)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(i) May require a Handling Operator to report or submit materials regarding its handling of Personal Information, enter offices or other places for investigation, make inquiries and check records or other documents (Article 40).</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(ii) May require an Authorised Entity for Protection of Personal Information to report its activities (Article 56).</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(i) May render a Handling Operator guidance or advice to a Handling Operator (Article 41).</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fined of up to 300,000 yen (Article 85); If the breach is committed by a person who is employed by an entity, such entity will be subject to the same fine (Article 87).</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Not applicable.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Same as above</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

16.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?

In relation to the PPC’s powers stated in question 16.1 above, the PPC would have the power to issue an order to ban a particular processing activity without need of a court order.

16.3 Describe the data protection authority’s approach to exercising those powers, with examples of recent cases.

Publicly available information does not enable the identification of specific enforcement cases by the PPC since May 2017, when the PPC became the regulator and enforcement authority of the APPI. We are aware, though, that the PPC has initiated enforcement actions. However, there is not enough available information to allow a description of the PPC’s approach to the exercise of its powers.

16.4 Does the data protection authority ever exercise its powers against businesses established in other jurisdictions? If so, how is this enforced?

The enforcement powers by PPC against foreign companies have been newly introduced by the Amended APPI. Among the enforcement measures stated in question 16.1, the PPC’s enforcement power is limited to (i) rendering guidance or advice to a Handling Operator (Article 41), and (ii) recommending a Handling Operator to cease the violation and take other necessary measures to correct the violation (Article 42.1).

17 E-discovery / Disclosure to Foreign Law Enforcement Agencies

17.1 How do businesses typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?

Under the APPI, the general rule is that the Handling Operator cannot provide Personal Data to any “third party” without obtaining the prior
consent of the principal, except in specified cases (Article 23.1). These specified cases are cases where the provision of Personal Data is:

(i) required by laws and regulations;
(ii) necessary to protect the life, body, or property of a person and it is difficult to obtain the consent of the principal;
(iii) necessary to improve public health and promote the sound nurturing of the young and it is difficult to obtain the consent of the principal; and/or
(iv) necessary for governmental bodies to perform their business and getting the consent of the principal will likely impede the proper performance of business.

It is understood that “governmental bodies” referenced in (iv) above would be bodies of the Japanese government and not of other countries, and “laws” referenced in (i) above would not include foreign laws. If the Handling Operator were compelled to disclose Personal Information of Japanese individuals in accordance with a foreign law or by an action of a foreign governmental institution, the Handling Operator may be able to disclose the personal data in accordance with (ii) above; however, to avoid any risk in this regard, it is practical to obtain the prior consent of the data owners before transferring data in response to requests from foreign law enforcement agencies.

17.2 What guidance has/have the data protection authority(ies) issued?

There is no specific guidance by PPC regarding the response to foreign e-discovery requests or requests for disclosure from foreign law enforcement agencies.

18 Trends and Developments

18.1 What enforcement trends have emerged during the previous 12 months? Describe any relevant case law.

As per questions 1.1 and 1.4, the PPC, as an independent regulatory body, has the authority to enforce the PPC as of May 30, 2017. The enforcement cases brought by the PPC regarding the APPI in FY 2017 (April 2017 to March 2018) are: 305 cases where the PPC required Handling Operators to report or submit materials regarding their handling of Personal Information; and 270 cases where the PPC rendered the guidance or advices. The enforcement cases in the first half of FY 2018 (April 2018 to September 2018) were: two cases where the PPC entered offices or other places for investigation; 211 cases where the PPC required Handling Operators to report or submit materials regarding their handling of Personal Information; and 139 cases where the PPC rendered guidance or advice.

18.2 What “hot topics” are currently a focus for the data protection regulator?

The APPI contains a provision that it will be reviewed three years after taking effect and, if necessary, it may be amended. 2020 is the year when the APPI will be subject to such regular review. The PPC is discussing the amendment of the APPI, and considering the possibility of ensuring the proper handling of the information of users in connection with the expansion of platform services. The discussion includes the possibility of introducing a “right to be forgotten”, as well as stricter rules on the leakage of Personal Data.

Mori Hamada & Matsumoto

Mori Hamada & Matsumoto is a full-service international law firm based in Tokyo with offices in Bangkok, Beijing, Shanghai, Singapore and Yangon, with a desk in Indonesia. The firm has over 400 attorneys and a support staff of approximately 450 people, including legal assistants, translators and secretaries. The firm is one of the largest law firms in Japan and is particularly well-known in the areas of mergers and acquisitions, finance, litigation, insolvency, telecommunications, broadcasting and intellectual property, as well as domestic litigation, bankruptcy, restructuring and multi-jurisdictional litigation and arbitration. The firm regularly advises on some of the largest and most prominent cross-border transactions, representing both Japanese and foreign clients. In particular, the firm has extensive practice in, exposure to and expertise on telecommunications, broadcasting, internet, information technology and related areas, and provides legal advice and other legal services regarding the corporate, regulatory, financing and transactional requirements of clients in these areas.

Hiromi Hayashi

Hiromi Hayashi is a partner at Mori Hamada & Matsumoto, which she joined in 2001. She specialises in communications law and regulation and authored the Japanese section of Telecommunication in Asia in 2005. Her other areas of practice are international and domestic transactions, takeover bids and corporate restructuring. Hiromi was admitted to the Bar in 2001 in Japan and in 2007 in New York. She worked at Mizuho Corporate Bank from 1989 to 1994 and at Davis Polk & Wardwell in New York from 2006 to 2007.
Chapter 26

Korea

Lee & Ko

1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

In Korea, the collection and processing of personal data is governed by the Personal Information Protection Act ("PIPA"), the comprehensive general data protection law.

1.2 Is there any other general legislation that impacts data protection?

The Criminal Code makes it a criminal offence for any party to open any letter, document or drawing that is sealed or designed to be secret, or to learn the contents of any such letter, document, drawing, or special recording medium such as electronic records by employing technical means.

The Communications Privacy Protection Act ("CPPA") makes it a criminal offence for any party to acquire or record the contents of any "transmission or reception of all kinds of sounds, words, symbols or images by wire, wireless, fibre-optic cable or other electromagnetic system, including telephone [and] e-mail", except with the consent of the party concerned.

1.3 Is there any sector-specific legislation that impacts data protection?

There are a number of other sector-specific laws which include:

- the Act on Promotion of Information and Communications Network Utilisation and Information Protection (the “Network Act”), which governs information and communications service providers;
- the Utilisation and Protection of Credit Information Act (the “Credit Information Act”) and the Electronic Financial Transactions Act, both of which protect consumer financial information; and
- the Act on the Protection and Use of Location Information (the “Location Information Act”), which protects personal location information.

1.4 What authority(ies) are responsible for data protection?

- MOIS (Ministry of the Interior and Safety): enforces the PIPA and issues formal interpretations thereon.
- PIPC (Personal Information Protection Commission): shapes data protection policy while assessing the enactment/amendment of laws and administrative measures relating to the protection of personal information.
- KCC (Korea Communications Commission): enforces the Network Act and issues formal interpretations thereon.
- KISA (Korea Internet & Security Agency): performs tasks delegated to it by the MOIS, KCC and PIPC.
- FSC (Financial Services Commission): enforces the Credit Information Act and issues formal interpretations thereon.

2 Definitions

2.1 Please provide the key definitions used in the relevant legislation:

- “Personal Data”
  Under the PIPA, “personal data” is defined as “any data relating to a living person, and from which the individual can be identified through one’s name, resident registration number, or visual image and so on (including information which, if not by itself, can be easily combined with other information to identify a specific individual)”.

- “Processing”
  Under the PIPA, “processing” is defined as “the collection, generation, recording, storage, retention, processing, editing, search, outputting, rectification, restoration, use, provision, disclosure or destruction of personal information or any other action similar to any of the foregoing”.

- “Controller”
  Under the PIPA, “data controller” means “a public institution, corporate body, organisation, or individual who processes information directly or via another person to administer personal information files (defined as “a collection of personal information in which personal information is systematically organised pursuant to certain rules for easy search/use”) as part of its/his/her duties”.

The Network Act regulates the processing of personal data of users by information and communications service providers ("ICSps") which are defined as “(1) telecommunications business operators under the Telecommunications Business Act and (2) commercial providers of information services that utilise telecommunications services provided by a telecommunications business operator".

Under the Credit Information Act, the concept of “credit information provider/user” is similar to that of a controller and means “a person who provides any third party with credit..."
information obtained or produced in relation to his/her own business for purposes of commercial transactions, such as financial transactions with customers, or who has been continuously supplied with credit information from any third party to use such information for his/her own business, or other persons corresponding thereto.

- **“Processor”**
  Under the PIPA, an “outsourced processor” means “a public institution, corporate body, organisation, or individual who processes personal information entrusted by and for the benefit of the data controller”.

- **“Data Subject”**
  Under the PIPA, a “data subject” means “a person who can be identified by processed information and therefore is the subject of the given piece of information”.

  Under the Network Act, a “user” means “a person who uses information and communications services provided by an ICSP”.

- **“Sensitive Personal Data”**
  Under the PIPA and regulations issued thereunder, “sensitive personal data” means any information on the ideology, creed, membership of a labour union or political party, political views, health, sexual preferences, bio-data, and criminal records as defined under the Act on the Lapse of Criminal Sentences.

- **“Data Breach”**
  Under the Standard Guidelines for the Protection of Personal Data, a “personal information leak” is defined as “the data controller’s involuntary loss of control of the personal data of data subjects or the allowance of access thereto by unauthorised persons that is not pursuant to an applicable law or regulation”.

  **Other key definitions – please specify (e.g., “Pseudonymous Data”, “Direct Personal Data”, “Indirect Personal Data”)**

- **“Particular Identification Data”:** unique identifiers assigned to each individual as prescribed by law or regulation such as resident registration numbers (“RRNs”), driver’s licence numbers, passport numbers, and alien registration numbers.

- **“Pseudonymised Data”:** although this concept is not currently defined under the current regime, proposed amendments to the PIPA and the Credit Information Act containing definitions of this concept (based on the definition under the EU data protection regime) have been introduced in the National Assembly and are currently under review.

## 3 Territorial Scope

### 3.1 Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to those laws?

Although Korean data protection laws do not expressly provide as such, regulators in Korea are of the position that Korean data protection laws should also apply to foreign companies without a business presence in Korea (“Foreign Companies”) that process the personal data of Korean citizens. Following recent amendments to the Network Act in 2018, ICSPs that are Foreign Companies meeting any of the following criteria will be required to designate a Korean representative to handle various tasks related to the processing of personal data (e.g., perform responsibilities as the Data Protection Officer, perform notification/report obligations following any leakages of personal data, submit necessary information during investigations): (i) recorded revenue of at least KRW 1 trillion for the previous (fiscal) year; (ii) recorded revenue of at least KRW 10 billion in the information and communications sector for the previous (fiscal) year; (iii) stored or managed the personal data of a daily average of at least 1 million users during the last three months of the previous (fiscal) year; or (iv) received a request for information from the KCC in response to an actual or potential data breach involving personal data.

## 4 Key Principles

### 4.1 What are the key principles that apply to the processing of personal data?

- **Transparency**
  The data controller shall disclose matters related to the processing of personal data (e.g., through a privacy policy), and guarantee the data subject’s right to access his/her personal data.

- **Lawful basis for processing**
  The data controller must lawfully and justly collect personal data.

- **Purpose limitation**
  The data controller shall make clear the purposes of processing personal data, properly process the personal data within the scope of such purposes, and shall not use the personal data for any other purpose.

- **Data minimisation**
  The data controller shall collect only the minimum amount of personal data that is necessary for carrying out its stated purposes and the data controller shall bear the burden of proving that its collection of personal data adheres to this minimum necessary standard.

- **Proportionality**
  The data controller shall properly process the personal data within the scope of the purpose necessary for processing the personal data.

- **Retention**
  The data controller shall safely manage the personal data by taking into consideration the likelihood/risk of the data subject’s rights being infringed upon based on the method and type of processing.

  The data controller shall implement managerial, technical, and physical security measures necessary to ensure the safety of personal data and destroy personal data without delay as soon as it is no longer necessary.

  **Other key principles – please specify**

- **Restriction on the processing of RRNs**: Under the PIPA, data controllers may not collect or use RRNs except in the following cases:
  1. the processing of RRNs is specifically required or permitted by a law or regulation; or
  2. there exists a clear and urgent need to protect the life, physical or economic interest of the data subject or a third party.

  Following recent amendments to the Network Act and Location Information Act in 2018, the following requirements are also applicable when processing personal data and personal location data of data subjects under the age of 14: (i) ICSPs must use easily understandable formats and language when providing notice of matters related to personal data to data subjects under the age of 14; and (ii) ICSPs, location information business operators, location-based service providers, and any other parties seeking to process the personal (location) data of data subjects under the age of 14 must obtain consent from and verify the consent of the legal guardians of such underage data subjects.
5 Individual Rights

5.1 What are the key rights that individuals have in relation to the processing of their personal data?

- **Right of access to data/copies of data**
  A data subject is entitled to request access to his/her personal data that is being processed by a data controller and the data controller must comply with the data subject’s request within 10 days of receiving such request unless it has a justifiable reason.

- **Right to rectification of errors**
  Once the data subject accesses his/her personal data, such data subject has the right to request the data controller to rectify his/her personal data and in such cases, the data controller is required to review the subject personal data without delay and provide notice of the status/results of the data subject’s request, after taking necessary measures such as rectification.

- **Right to deletion/right to be forgotten**
  Once the data subject accesses his/her personal data, such data subject has the right to request the data controller to delete his/her personal data and in such cases, the data controller is required to review the subject personal data without delay and provide notice of the status/results of the data subject’s request, after taking necessary measures such as deletion.

- **Right to object to processing**
  A data subject is entitled to request the suspension of the processing of his/her personal data that is being processed by a data controller and the data controller must, without delay, suspend processing of some or all of the data subject’s personal data unless it has a justifiable reason.

- **Right to restrict processing**
  Individuals do not appear to have the right to restrict processing. However, the Network Act provides that ICSPs, upon receiving requests from users to rectify errors in their personal data, must refrain from using or providing such personal data until necessary measures have been taken.

- **Right to data portability**
  There is no right to data portability under Korean law, but proposed amendments to the Credit Information Act, creating a right to data portability (based on the definition under the EU data protection regime) for personal credit information, have been introduced in the National Assembly and are currently under review.

- **Right to withdraw consent**
  Although the PIPA does not expressly provide the right to withdraw consent, it is widely understood that this right is implied thereunder because data subjects are entitled to choose whether to provide consent, and to determine the scope of such consent.

- **Right to object to marketing**
  When obtaining consent for the processing of personal data for the purpose of promoting goods/services or soliciting the sale thereof, the data controller shall provide clear notice of such purpose to data subjects, and the data controller may not deny the subject goods/services to a data subject that has refused his/her consent to the such purpose.

- **Right to complain to the relevant data protection authority(ies)**
  Any person who suffers infringement of rights or interests relating to his/her personal data, when such personal data is processed by a data controller, may report such infringement to KISA. Any person who wants a dispute over personal data to be mediated, may apply to the Dispute Mediation Committee for mediation of such dispute.

**Other key rights – please specify**

- **Liability related to the processing of personal data**
  Under the PIPA, a data controller may not avoid liability for damages arising from the leakage or misuse of personal data it has processed for its own benefit, unless it can establish that such leakage or misuse is not attributable to its intentional or negligent act or omission. In the event a data subject suffers damages due to the loss, theft, leakage, falsification, alteration, or damage of his/her own personal data caused by an intentional or grossly negligent act or omission of the data controller, a court may award punitive damages of up to treble the amount of suffered damages. The PIPA also provides that statutory damages of up to KRW 3 million may be awarded under certain conditions even if the data subject is unable to prove the actual amount of suffered damages.

6 Registration Formalities and Prior Approval

6.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?

In general, businesses (excluding public institutions) are not subject to any registration/notification obligations when processing personal data. However, businesses handling specific information (which typically includes personally identified/identifiable information) may become subject to certain registration/notification obligations for their businesses.

Any person who intends to operate a location information business that processes the location information of individuals must obtain permission from the KCC after indicating his/her trade name, location of the main office, type and description of the relevant location information business, and major business facilities, including location information systems. Any person who intends to operate a location information business that processes the location information of objects must file a report with the KCC indicating his/her trade name, the location of the main office, the type of the relevant location information business, and major business facilities, including location information systems. Any person who intends to operate a location-based service business (excluding those not processing personal location data) must file a report with the KCC indicating his/her trade name, the location of the main office, the type of relevant location-based service business, and major business facilities, including location information systems. Under the Credit Information Act, any person who intends to operate a credit inquiry rating service, credit investigation service, etc. (which typically handle credit information) must obtain permission from the FSC.

6.2 If such registration/notice is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?

Any person who intends to obtain permission to operate a location information business that processes the location information of individuals shall file an application form that includes detailed
information on the following, in addition to a business plan: 1) general information regarding the applying corporation; 2) a sales plan; and 3) a technical plan.

Any person who intends to file a report as a location information business that processes the location information of objects shall include the following documents: 1) a business plan; 2) documents describing and indicating the location of major business facilities; and 3) documents confirming the implementation of security measures for location information.

Any person who intends to file a report as a location-based service business shall include the following documents: 1) a business plan; 2) documents describing and indicating the location of major business facilities; and 3) documents confirming the implementation of security measures for location information.

6.3 On what basis are registrations/notifications made (e.g., per legal entity, per processing purpose, per data category, per system or database)?

Please refer to our response to question 6.1.

6.4 Who must register with/notify the data protection authority (e.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation)?

The KCC has recently begun enforcing the location-based service report filing requirement against Foreign Companies, whereas previously it did not require location-based service reports of Foreign Companies, even if they were theoretically required to do so under the Location Information Act. As a result, many Foreign Companies are in the process of preparing and filing their location-based service reports.

6.5 What information must be included in the registration/notification (e.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes)?

Please refer to our response to question 6.2.

6.6 What are the sanctions for failure to register/notify where required?

Any person who operates a location information business that processes the location information of individuals, without obtaining registration, may be subject to imprisonment of up to five years or a fine of up to KRW 50 million.

Any person who operates a location information business that processes the location information of objects or a location-based service business that processes personal location data, without filing a report, may be subject to imprisonment of up to three years or a fine of up to KRW 30 million.

6.7 What is the fee per registration/notification (if applicable)?

This is not applicable in Korea.

6.8 How frequently must registrations/notifications be renewed (if applicable)?

This is not applicable in Korea. For your reference, there is no expiration date for registrations/notifications.

6.9 Is any prior approval required from the data protection regulator?

Please refer to our response to question 6.1.

6.10 Can the registration/notification be completed online?

Yes, but the relevant website is only provided in Korean.

6.11 Is there a publicly available list of completed registrations/notifications?

Such information is maintained by the KCC, available at the following link (only in Korean): https://kcc.go.kr/user.do?boardId=1030&page=A02060400&dc=K02060400.

7 Appointment of a Data Protection Officer

7.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.

Under the PIPA, the appointment of a Data Protection Officer (“DPO”) is mandatory. That said, ICSPs who have appointed a DPO as required under the Network Act will be exempted from the requirement to appoint a DPO under the PIPA (any other requirements in this section 7 that are applicable under both the PIPA and Network Act will be explained from the perspective of the PIPA unless indicated otherwise).

Recent amendments to the Network Act now require ICSPs exceeding a certain size to appoint an executive-officer-level Chief Information Security Officer (“CISO”) and report such fact to the Ministry of Science and ICT (“MSIT”) (please refer to question 18.2 for further details).

7.2 What are the sanctions for failing to appoint a Data Protection Officer where required?

Failure to appoint a DPO may result in an administrative fine of up to KRW 10 million. ICSPs that fail to appoint a DPO, as required under the Network Act, may face an administrative fine of up to KRW 20 million.
7.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect of his or her role as a Data Protection Officer?

A data controller may not permit a DPO to suffer any disadvantages when performing his/her duties, without a justifiable reason.

7.4 Can a business appoint a single Data Protection Officer to cover multiple entities?

The PIPA does not expressly prohibit the appointment of a single DPO to cover multiple entities. However, we are not aware of any cases where a DPO has been appointed as such.

7.5 Please describe any specific qualifications for the Data Protection Officer required by law.

The PIPA provides that the DPO must be the owner of the business, representative director, executive officer, or (if there are no executive officers) the head of the department responsible for handling tasks related to the processing of personal data. The Network Act provides that the DPO must be an executive officer or the head of the department responsible for handling tasks related to the processing of personal data.

7.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?

The DPO is responsible for the overall management of tasks related to the processing of personal data and performs the following specific tasks: 1) establishes and executes a personal data protection plan; 2) carries out routine check-ups and improves the conditions and practices concerning the processing of personal data; 3) responds to relevant complaints, and provides redress to data subjects who have incurred damages from such processing; 4) establishes an internal control system to prevent leakages, misuse and abuse of personal data; 5) establishes and implements education programmes; 6) protects, manages and supervises personal data files; 7) establishes, modifies and executes a privacy policy; 8) manages materials relating to the protection of personal data; and 9) destroys personal data whose retention period has expired or for which the purposes of processing have been achieved.

7.7 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?

No, the appointment of a DPO does not have to be registered or notified.

7.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?

Yes. In the event a DPO has been appointed or replaced, confirmation of such fact and the name, department, and contact information of relevant individuals must be disclosed in the privacy policy.

8 Appointment of Processors

8.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?

Yes. Under the PIPA, in order to outsource the processing of personal data to third parties, data controllers are required to enter into a written data processing agreement with the outsourced processor that includes the following matters stipulated by law: 1) restrictions on the processing of personal data beyond the purposes of the outsourced tasks; 2) matters related to technical and managerial security measures for the protection of personal data; 3) the purposes and scope of the outsourced tasks; 4) restrictions on the subcontracting of the outsourced tasks; 5) measures to ensure the security of personal data such as restriction of access; 6) matters related to supervision of the outsourcing of the processing of personal data; and 7) matters related to the data controller’s liability for damages that may arise due to violations committed by outsourced processors.

8.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?

Please refer to our response to question 8.1.

9 Marketing

9.1 Please describe any legislative restrictions on the sending of electronic direct marketing (e.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?).

Under the Network Act, the transmission of for-profit advertisements through an electronic medium (e.g., telephone, mobile phone, fax, email, etc.) requires the express prior consent of recipients. Additionally, the Network Act provides for certain information that must be included in for-profit advertisements and specifies certain acts that the sender is prohibited from engaging in.

9.2 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.).

A telemarketer, as defined under the Act on Door-to-Door Sales, Etc., may engage in telemarketing without obtaining the prior consent of recipients in cases where notice of the sources from which personal data is collected is provided orally to such recipients.

9.3 Do the restrictions noted above apply to marketing sent from other jurisdictions?

Although the above restrictions do not appear to be typically enforced on marketing sent from other jurisdictions, we are aware that the KCC has joined UCENET (Unsolicited Communications Enforcement Network), an international spam enforcement cooperation organisation, and is seeking to increase cooperation with other foreign enforcement agencies.
9.4 Is/are the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?

Among Korean regulators, the KCC and KISA actively enforce illegal spamming. KISA operates an illegal spam response centre that reviews illegal spam incidents upon receiving complaints and may request other enforcement agencies to conduct investigations and impose sanctions.

9.5 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?

Generally, no. However, the PIPA requires a data controller to obtain consent for the provision of personal data to third parties after providing data subjects with notice of certain matters regarding the provision. It is worth noting that the Supreme Court of Korea found that the defendant, a large retailer that operated a chain of discount stores, was criminally liable for violating the PIPA because it had acquired personal data or obtained consent for the processing of personal data by fraud or other unlawful means when it misled customers into believing they were participating in a promotional giveaway event and collected personal data that was unrelated to the event that was later sold to third parties for profit.

9.6 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?

Under the Network Act, any person that sends marketing communications through prohibited means (e.g., using measures to avoid or interfere with a recipient’s refusal to receive or withdraw his/her consent to the receipt advertising information, using measures to automatically generate a recipient’s contact information, etc.) or containing prohibited content (e.g., gambling, illegal drugs, etc.) may be subject to imprisonment for up to one year or a fine of up to KRW 10 million.

10 Cookies

10.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).

The law does not prescribe any particular rules relating to the use of cookies or equivalent technologies. To the extent any such information is deemed personal data, rules under the PIPA and the Network Act will apply. For your reference, ICSPs are required under the Network Act to disclose in their privacy policies information on the installation of applications (e.g., cookies) that automatically collect personal data, and the methods used to avoid such installation.

10.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?

This is not applicable in Korea.

10.3 To date, has/have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?

No enforcement action has been taken in relation to cookies.

10.4 What are the maximum penalties for breaches of applicable cookie restrictions?

This is not applicable in Korea.

11 Restrictions on International Data Transfers

11.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.

Korean law provides separate requirements for the provision of personal data (“Provision”) and the outsourcing of the processing of personal data (“Outsourcing”). Specifically, a Provision refers to cases where a data transfer is conducted for the benefit and business purpose of the transferee, whereas an Outsourcing refers to cases where a data transfer is conducted for the benefit and business purpose of the transferor.

Under the PIPA, if a data controller conducts a Provision to a foreign-based entity, it is required to obtain the consent of data subjects after providing notice of matters prescribed by law. However, if a data controller conducts an Outsourcing to a foreign-based entity, the data controller is not required to obtain such consent.

Under the Network Act, an ICSP that conducts a Provision or an Outsourcing to a foreign-based entity will be subject to notice and consent requirements. However, an ICSP is not required to obtain the consent of users if (i) an Outsourcing is necessary for the provision of service to users, (ii) it enhances the convenience of the users, and (iii) information such as the outsourced tasks and the identity of outsourced processors has been disclosed through the ICSP’s privacy policy. Following recent amendments to the Network Act in 2018, ICSPs will be required, in principle, to obtain consent from the data subject for the onward Provision or Outsourcing of his/her personal data to a third country after it is initially Provided or Outsourced from Korea.

11.2 Please describe the mechanisms businesses typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).

Personal data is normally transferred abroad after the data subjects’ consent is granted.

11.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.

There are no registration/notification requirements.
12 Whistle-blower Hotlines

12.1 What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?

There are no data protection rules governing whistleblowing, so the PIPA will be applicable as the general data protection law. However, it may be worth noting that the Protection of Public Interest Whistleblowers Act (“PPIWA”) provides for certain measures to be taken to ensure the secrecy and confidentiality of “public interest whistleblowers”. “Public interest whistleblowing” is defined as “reporting, petitioning, informing or accusing that a public interest violation (i.e., an act that infringes on the health and safety of the public, the environment, or consumer interests and fair competition, etc.) has occurred or is likely to occur, or the providing of information during an investigation of an alleged public interest violation”. Any person may report a public interest violation to the relevant organisation representative, an investigative agency, etc.

A public interest whistleblower must file a written report containing the personal details of the whistleblower and identity of person that is alleged to have committed a public interest violation. Under the PIPA, a public interest whistleblower is permitted to report the personal data of a person that is alleged without such person’s consent because such provision is specifically required under the PPIWA.

12.2 Is anonymous reporting prohibited, strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do businesses typically address this issue?

No, anonymous reporting is not prohibited. However, under the PPIWA, a public interest whistleblower must state his/her personal details when filing a written report in order to be afforded protection thereunder.

13 CCTV

13.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?

In general, there is no registration/notification requirement or need to obtain prior approval from the data protection authorities in order to use CCTV in Korea. However, a notice sign stating the following information must be placed in cases where CCTV is installed in a publically disclosed location: installation location and purpose of installation; field of view and recording time; person in charge of managing the CCTV and his/her contact information; and name (job title) of person in charge, name of company, and contact information of the outsourced third party (if applicable).

The prior consent of data subjects is required under the PIPA in order to lawfully install and operate CCTV in undisclosed locations.

13.2 Are there limits on the purposes for which CCTV data may be used?

If CCTV data can be used to identify specific individuals, then it will be regarded as personal data under the PIPA and the collection/use thereof will be subject to consent requirements thereunder. CCTV in undisclosed locations may only be installed and operated with the prior consent of data subjects.

In principle, the installation and operation of CCTV in a publicly disclosed location is prohibited under Korean law except in the following cases: where specially permitted by a law or regulation (e.g., parking lots, kindergartens, elementary schools, airports, etc.); where necessary to prevent crime or provide assistance to an investigation; where necessary for the safety of facilities or to prevent fires; where necessary for traffic regulation; and where necessary to collect, analyse, and provide traffic information.

14 Employee Monitoring

14.1 What types of employee monitoring are permitted (if any), and in what circumstances?

In general, employee monitoring is only permitted in cases where necessary consent has been obtained under the PIPA or CPPA. Please note, however, that in a case where a company conducted employee monitoring based on reasonable suspicions that the confidential information of the company was being leaked, the Supreme Court of Korea found that the company was justified in conducting employee monitoring.

14.2 Is consent or notice required? Describe how employers typically obtain consent or provide notice.

Yes, consent is required. The CPPA prohibits the wiretapping of a device without the consent of the party concerned. Also, there may be the issue of whether there was an invasion of such individual’s privacy in violation of the Criminal Code and the Network Act, and as employee monitoring will be deemed to be the collection of personal data, consent for the collection and use of personal data must be obtained in accordance with the PIPA. As the PIPA prescribes detailed rules on how to obtain the consent thereunder, it is necessary to obtain consent pursuant to the PIPA.

14.3 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?

The Act on the Promotion of Workers Participation and Cooperation provides that the work council shall be consulted with in order to “install employee surveillance systems/facilities within the workplace”.

15 Data Security and Data Breach

15.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?

Under the PIPA and Network Act, all data controllers (including data processors) are required to ensure the security of personal data. The Standards of Personal Information Security Measures, an implementing regulation issued under the PIPA; and the Standards of Technical and Administrative Safeguards for Personal Information, an implementing regulation issued under the Network Act, provide detailed information on security measures that must be implemented.
15.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

Yes. Under the PIPA, the MOIS must be notified if a data breach occurs that involves the personal data of 1,000 or more data subjects. Such notice should contain the items of personal data that have been leaked; the time when the personal data was leaked and reasons for the leak; information on measures to be taken by the data subject to minimise damages; countermeasures taken by the data controller and procedures for remedying damages to the data subject; and contact information for the data controller’s department responsible for reporting damages to the data subject. The PIPA provides that notification should be made “without delay”, which is interpreted as meaning “within five days” under regulatory guidelines.

In cases where the Network Act is applicable, the KCC must be notified, without delay (in any event, within 24 hours), upon the occurrence of a data breach unless there is a justifiable reason (there is no threshold of “1,000 or more data subjects”). The information that must be included when providing notification is identical to that provided by the PIPA.

15.3 Is there a legal requirement to report data breaches to affected data subjects? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

Yes, there is a legal requirement to report data breaches to affected data subjects. The information that must be included is identical to the information required when providing notification to data protection authorities. And, where the PIPA is applicable, data subjects must be notified even if the data breach affects fewer than 1,000 data subjects.

15.4 What are the maximum penalties for data security breaches?

The maximum penalties that may be imposed on each entity are as follows:

- A data controller that fails to implement security measures discussed in our response to question 15.1: an administrative fine of up to KRW 30 million.
- The person responsible for a failure to implement security measures discussed in our response to question 15.1 which leads to the loss, theft, leakage, falsification, alteration, or damage of personal data: imprisonment of up to two years or a fine of up to KRW 20 million.
- A data handler whose legal representative or employee is responsible for such failure to implement the security measures above: a fine of up to KRW 20 million.
- A data controller who is at fault for the leakage of RRNs it has been processing: a penalty surcharge of up to KRW 500 million.

16 Enforcement and Sanctions

16.1 Describe the enforcement powers of the data protection authority(ies).

<table>
<thead>
<tr>
<th>Investigatory Power</th>
<th>Civil/Administrative Sanction</th>
<th>Criminal Sanction</th>
</tr>
</thead>
<tbody>
<tr>
<td>MOIS</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>KCC</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>FSC</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Public Prosecutors</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

16.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?

The MOIS, KCC and FSC possess discretionary authority to issue bans (i.e., corrective orders) pursuant to applicable laws and such bans do not require a court order.

16.3 Describe the data protection authority’s approach to exercising those powers, with examples of recent cases.

Data protection authorities tend to exercise their powers actively. Specifically, the authorities will investigate reported violations and leakages of personal data, and may also investigate companies within a particular industry to identify and punish violations.

On March 28, 2018, the KCC imposed a penalty surcharge of KRW 112 million and an administrative fine of KRW 10 million against a security company, in connection with a data breach occurrence that resulted in the leakage of personal data.

On July 4, 2018, the KCC imposed a penalty surcharge of KRW 219 million and an administrative fine of KRW 10 million against a college admission test preparation company, in connection with a data breach occurrence that resulted in the leakage of personal data.

On February 6, 2018, the MOIS imposed a penalty surcharge of KRW 327 million and an administrative fine of KRW 10 million against a security company, in connection with a data breach occurrence that resulted in the leakage of personal data.

From August 20, 2018 until August 31, 2018, the MOIS conducted on-site inspections of the Korean subsidiaries of 20 major global companies (selected on the basis of revenue and other factors) to assess their compliance with data privacy requirements such as restriction of access and access authorisation for the personal data processing system, storage of access records for the personal data processing system, encryption of files containing personal data, destruction of personal data, and observing due process when conducting cross-border transfers of personal data.

16.4 Does the data protection authority ever exercise its powers against businesses established in other jurisdictions? If so, how is this enforced?

Yes. Most notably: 1) the KCC requested Facebook to upgrade its services based on the fact that they lacked the necessary protection for personal data (e.g., Facebook’s notification and consent procedures
were found to be inadequate), and Facebook announced its plans to improve upon its services before it was actually sanctioned by the KCC; and 2) the KCC also imposed penalty surcharges on Google Inc. (based in the US) for collecting personal data without obtaining the data subject’s consent in connection with Google’s provision of Street View services.

17 E-discovery / Disclosure to Foreign Law Enforcement Agencies

17.1 How do businesses typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?

Korean laws do not provide any particular rules on third-country e-discovery or law enforcement requests. Therefore, personal data that is provided to a foreign regulatory authority or judicial authority will be treated the same as personal data that is provided to a third party.

17.2 What guidance has/have the data protection authority(ies) issued?

There has been no relevant guidance issued.

18 Trends and Developments

18.1 What enforcement trends have emerged during the previous 12 months? Describe any relevant case law.

Recently, the focus of enforcement has been expanded to security measures for personal data. As discussed in our response to question 16.3, the KCC has recently imposed stern administrative sanctions for data breaches.

18.2 What “hot topics” are currently a focus for the data protection regulator?

In November 2018, a number of bills amending the PIPA, the Network Act, the Location Information Act, and the Credit Information Act were introduced in the National Assembly and are currently under review. Notably, the bill amending the PIPA seeks to: (i) introduce the concept of ‘pseudonymised data’; (ii) expand the permissible purposes for the processing of personal data; (iii) permit the processing of pseudonymised data without consent for statistical purposes, scientific research purposes, or archiving purposes in the public interest; and (iv) permit the combination of data sets of two or more data handlers. Furthermore, enforcement powers granted separately to the KCC and the MOIS will be combined and transferred to the Personal Information Protection Committee. It is also worth noting that the Korean government is expected to undergo an adequacy assessment under the GDPR, in consultation with the EU Commission, after the bill amending the PIPA passes the National Assembly.

Meanwhile, once the 2018 amendments to the Network Act (discussed in the preceding sections) take effect on June 13, 2019: (1) ICSPs will be required to appoint an executive-officer-level CISO and report such fact to the MSIT (however, ICSPs meeting certain criteria prescribed by the Enforcement Decree of the Network Act relating to total assets, annual revenue, or other characteristics will be exempted from this requirement); and (2) ICSPs meeting certain criteria prescribed by the Enforcement Decree of the Network Act will be required to obtain liability insurance, mutual aid, or set aside reserves to prepare against damages caused by violations of the Network Act related to data protection.

Corresponding amendments to the Enforcement Decree of the Network Act – stipulating the various criteria mentioned above – have yet to be enacted, as the MSIT has just recently concluded a public review and comment period for its proposed amendments (set forth below) and thus, the relevant provisions may undergo further changes prior to enactment.

- The following parties will be exempted from requirement (1) (i.e., appointment of executive-officer-level CISO): (a) parties intending to operate a small-scale value-added telecommunications business in accordance with the Telecommunications Business Act; (b) micro enterprises as defined under the Act on the Protection of and Support for Micro Enterprises; and (c) small enterprises (excluding telecommunications business operators and business operators of clustered information and communications facilities) who have recorded a daily average of fewer than 1 million users during the last three months of the previous year, and who have recorded revenue of less than KRW 10 billion in the information and communications service sector for the previous year.
- ICSPs who have stored or managed the personal data of a daily average of at least 1,000 users during the last three months of the previous year will be subject to requirement (2) (i.e., to obtain liability insurance, mutual aid, or set aside reserves).
Kwang Bae Park
Lee & Ko
Hanjin Building
63 Namdaemun-ro
Jung-gu
Seoul 04532
Korea
Tel: +82 2 772 4343
Email: kwangbae.park@leeko.com
URL: www.leeko.com

Kwang Bae Park is a partner and leader of the Technology, Media & Telecommunications Practice Group at Lee & Ko. He has consistently represented and advised various telecommunications and IT companies for more than 10 years since 1991, with a focus on various issues in the field of TMT, including mobile and regulatory issues in internet services, such as issues on privacy, internet content, and internet advertisements.

Mr. Park also serves on various committees such as the Regulation Review Committee (Ministry of Science and ICT), the Joint Task Force for EU Adequacy Assessment (Ministry of the Interior and Safety), etc. In addition, he was awarded and recognised as a “Leading Telecoms & Media Lawyer” (The International Who’s Who Legal, 2014–2017), a “ Ranked Lawyer” (Band 1) (Chambers Asia Pacific, 2015–2017), among other accolades.

Mr. Park holds an LL.B. from Seoul National University and an LL.M. from Georgetown University Law Center. He is admitted to the New York and Korean Bars.

Hwan Kyoung Ko
Lee & Ko
Hanjin Building
63 Namdaemun-ro
Jung-gu
Seoul 04532
Korea
Tel: +82 2 2191 3057
Email: hwankyoung.ko@leeko.com
URL: www.leeko.com

Hwan Kyoung Ko is a partner in the Technology, Media & Telecommunications Practice Group. He is a leading expert in the areas of telecommunications, IT, data privacy, and FinTech. He has advised numerous government agencies, including the Financial Services Commission and the Korea Communication Commission, on data protection and has also served as a member of the Big Data Task Force. Mr. Ko has also been involved in efforts to promote the Big Data industry in Korea, as witnessed by his participation in a recent Hackathon event hosted by the Presidential Committee on the Fourth Industrial Revolution.

Mr. Ko is a recipient of the 2019 Presidential Citation (for active involvement in the drafting of legislation to promote the Data Economy), the 2016 Minister of the Interior and Safety’s Award (in the data protection sector) and the 2014 KISA President’s Award for Personal Data Protection.

Mr. Ko holds a B.A. from Korea University and an LL.M. from Georgetown University Law Center. He is admitted to the New York and Korean Bars.

Lee & Ko’s evolution as the premier law firm in Korea parallels in many ways the solid economic development of the country for more than 40 years following its founding in 1977.

Our firm is one of the top law firms in Korea that is recognised for expertise in all major practice areas, which includes over 30 specialised practice groups, and that is consistently acclaimed over the years as one of the leading firms in Asia by internationally respected legal publications and league tables.

Also, Lee & Ko has a global client base that ranges from domestic conglomerates to multinational corporations in many different industries. We have an unrivalled list of leading clients from the US, EU, China, Japan and more, as well as high-profile, high-tech start-up companies. Our global reach is a result of our Korean-licensed lawyers with outstanding foreign-language capabilities working together with our experienced foreign-licensed lawyers.
Chapter 27

Kosovo

Deloitte Legal Shpk

1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

The principal legislation is as follows:


ii. Law no. 06/L-082, dated 30.01.2019 on Protection of Personal Data (hereinafter: “the Law”).

iii. The sub-legal acts enacted by the competent authority on personal data protection. These acts are issued prior to entering into the force of the new Law; however, as long as they do not contradict the present Law, they will remain in force until the issuance of the new sub-legal acts. The following acts are still in force:

■ Regulation no.01/2015, dated 23.01.2015 on the manner of storage and use of archive material and protocol.
■ Regulation no. 03/2015, dated 07.05.2015 on security measures in the course of personal data processing, as amended.
■ Regulation no.05/2015, dated 23.06.2015 on the manner of registering in the records of personal data filing systems and the pertinent record forms.

1.2 Is there any other general legislation that impacts data protection?

Rules impacting the personal data protection in Kosovo are also laid down, inter alia, in the following legislation:

■ Law no. 05/L -031 on General Administrative Procedure.
■ Law no. 06/L –085 on Protection of Whistle-blowers.
■ Law no. 04/L-076 on Police.
■ Law no. 04/L-003 on Civil Status.
■ Law no. 03/L –215 on Access to Public Documents.

1.3 Is there any sector-specific legislation that impacts data protection?

Law no. 04/L-109 on Electronic Communication contains several provisions related to the processing of personal data and the protection of privacy in the electronic communications sector.

1.4 What authority(ies) are responsible for data protection?

The competent authority is the Information and Privacy Agency (hereinafter: the “Agency”).

2 Definitions

2.1 Please provide the key definitions used in the relevant legislation:

■ “Personal Data”
Any information related to an identified or identifiable natural person (“data subject”); an identifiable natural person is one who can be identified directly or indirectly, particularly by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

■ “Processing”
Any operation or set of operations performed on personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

■ “Controller”
Any natural or legal person, public authority, agency or other body which, alone or jointly with others, determines purposes and means of personal data processing.

■ “Processor”
A natural or legal person, from the public or private sector, who processes personal data for and on behalf of the data controller.

■ “Data Subject”
A natural person who is subject to the relevant personal data.

■ “Sensitive Personal Data”
Personal data revealing ethnic or racial origin, political or philosophical views, religious affiliation, union membership or any data related to health condition or sexual life, any involvement in or removal from criminal or offence records retained in accordance with the law. Biometric characteristics are also considered sensitive personal data if the latter enable the identification of a data subject in relation to any of the abovementioned circumstances in this sub-paragraph.
“Data Breach”
A breach of security measures leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Other key definitions – please specify (e.g., “Pseudonymous Data”, “Direct Personal Data”, “Indirect Personal Data”)

Genetic Data: personal data relating to the inherited or acquired genetic characteristics of a natural person, which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question.

Biometric Data: all personal data resulting from specific processing related to physical, physiological or behavioural characteristics of an individual that allows or confirms the unique identification of that natural person, as well as visual images or dactyloscopic, psychological and behavioural data of all individuals but which are specific and permanent for each individual, if it can be used for identifying an individual, such as: fingerprints; finger papillary lines; iris; retina; facial features; and DNA.

3 Territorial Scope

3.1 Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to those laws?

The Law applies also to data controllers established in other jurisdictions, which, for the purpose of personal data processing, make use of automatic or other equipment in the Republic of Kosovo, unless such equipment is used only for purposes of transit through the territory of Kosovo. In such cases, controllers must designate a representative registered in Kosovo.

4 Key Principles

4.1 What are the key principles that apply to the processing of personal data?

- **Transparency**
  Personal data must be processed lawfully, fairly and in a transparent manner. The controller shall take the appropriate measures to provide any information related to the processing of personal data in a concise, transparent, intelligible and easily accessible form. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means.

- **Lawful basis for processing**
  Personal data shall be processed in an impartial, lawful and transparent manner, without infringing the dignity of the data subject.

- **Purpose limitation**
  Personal data are collected only for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purpose.

- **Data minimisation**
  Personal data shall be adequate, relevant and limited to the purposes for which they are further collected or processed.

The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed.

- **Proportionality**
  The principle of proportionality is not specifically addressed in the Law, but it is applied, inter alia, in harmony with the principles of purpose limitation and transparency.

- **Retention**
  The retention principle is enshrined under the principle of storage limitation. According to this principle, personal data may be stored insofar as necessary to achieve the purpose for which they are further collected or processed. After the fulfilment of processing purpose, personal data shall be erased, deleted, destroyed, blocked or anonymised, unless otherwise foreseen in the Law on State Archives or in another relevant law.

- **Other key principles – please specify**

  **Principle of accuracy**
  Personal data shall be accurate and kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

  **Principle of accountability**
  The controller shall be responsible for, and be able to demonstrate compliance with, all of the above principles.

5 Individual Rights

5.1 What are the key rights that individuals have in relation to the processing of their personal data?

- **Right of access to data/copies of data**
  The data subject shall have the right to obtain, from the controller, confirmation as to whether their personal data are being processed and, if so, to obtain from the controller, inter alia, the following information (right to access):
  a. the purpose of the processing;
  b. the categories of personal data concerned;
  c. the recipients or categories of recipient to whom the personal data have been or will be disclosed; in particular, recipients in third countries or international organisations;
  d. the envisaged period for which the personal data will be stored;
  e. the right to request the rectification or erasure of the personal data, as well as the right to submit a complaint to the Agency; and
  f. in the case of automated decisions, information about the logic applied in the decision-making process.

- **Right to rectification of errors**
  The data subject has the right to the rectification of inaccurate and/or incomplete personal data without undue delay.

- **Right to deletion/right to be forgotten**
  The data subject shall have the right to obtain from the data controller the erasure of personal data concerning him/her (the right to be forgotten). Following the request of a data subject, the controller is obliged to erase personal data without undue delay, where any of the below grounds applies:
  a. the personal data are no longer necessary for the purposes for which they were collected/processed;
b. the data subject objects to the processing of personal data and there are no overriding legitimate grounds for their processing;

c. the data subject withdraws the consent on which the processing is based;

d. the personal data have been unlawfully processed; or

e. there is a legal requirement to which the controller is subject.

■ Right to object to processing
The data subject has the right to object to the processing of personal data where the basis for that processing is either the public interest or legitimate interest of the controller or of a third party. The controller shall no longer process the personal data, unless the controller demonstrates compelling legitimate grounds for their processing, which overrides the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

■ Right to restrict processing
The data subject has the right to restrict the processing of personal data if:

a. the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of personal data;

b. the processing is unlawful and the data subject objects to the erasure and requests the restriction of processing instead;

c. the controller no longer needs the data for their original purpose, but the data are still required by the controller in order to establish, exercise or defend legal claims; or

d. the data subject has objected to processing pending verification as to whether the legitimate grounds of the controller override those of the data subject.

■ Right to data portability
The data subject shall have the right to receive the personal data concerning him/her, which he/she has provided to a controller, in a structured, commonly used and machine-readable format, and shall have the right to transmit those data to another controller, without hindrance from the controller to whom the personal data have been provided, where, inter alia:

a. the processing is based on the consent of the data subject; or

b. the processing is carried out by automated means.

■ Right to withdraw consent
The Law stipulates that the data subject is entitled to withdraw his/her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before such withdrawal.

■ Right to object to marketing
The provisions of the Law set out that where personal data are processed for direct marketing purposes, the data subject shall have the right to object, at any time, to the processing of personal data concerning him/her for such marketing, which includes profiling to the extent that it is related to such direct marketing.

■ Right to complain to the relevant data protection authority(ies)
Any person who claims that the rights, freedoms and legal interests concerning his/her personal data have been violated, is entitled to lodge a complaint with the Agency.

■ Other key rights – please specify
Data subjects can address the court and seek damage relief in cases of unlawful processing of personal data. Data subjects are also entitled to effective judicial remedy against a legally binding decision of the Agency, or in cases where the Agency does not address the data subject’s complaint or fails to inform the data subject on the progress or the outcome of the lodged complaint, as per the Law’s requirements.

6 Registration Formalities and Prior Approval

6.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?

The Law does not contain any obligation on businesses to register with the Agency or notify the latter in respect of their processing activities. However, the Law stipulates that the Agency issues certifications to controllers, processors as well as legal entities/enterprises, which process personal data. These certifications are issued based on the criteria and the procedures set out under a sub-legal act to be enacted by the Agency.

6.2 If such registration/notification is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?

Please refer to our answer to question 6.1.

6.3 On what basis are registrations/notifications made (e.g., per legal entity, per processing purpose, per data category, per system or database)?

Please refer to our answer to question 6.1.

6.4 Who must register with/notify the data protection authority (e.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation)?

Please refer to our answer to question 6.1.

6.5 What information must be included in the registration/notification (e.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes)?

Please refer to our answer to question 6.1.

6.6 What are the sanctions for failure to register/notify where required?

Please refer to our answer to question 6.1.

6.7 What is the fee per registration/notification (if applicable)?

Please refer to our answer to question 6.1.
6.8 How frequently must registrations/notifications be renewed (if applicable)?

Please refer to our answer to question 6.1.

6.9 Is any prior approval required from the data protection regulator?

No, there is no such requirement. However, as described in our answer to question 11.3 below, in case of transfer of personal data to other jurisdictions and/or international organisations without an adequate level of data protection, prior authorisation from the Agency is needed.

6.10 Can the registration/notification be completed online?

Please refer to our answer to question 6.1.

6.11 Is there a publicly available list of completed registrations/notifications?

This is not applicable.

6.12 How long does a typical registration/notification process take?

Please refer to our answer to question 6.1.

7 Appointment of a Data Protection Officer

7.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.

The Law obliges the controller and the processor to designate a Data Protection Officer (hereinafter: DPO) if:

a. the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;
b. the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, scope and/or purposes, require regular and systematic monitoring of data subjects on a large scale; or
c. the core activities of the controller or the processor consist of processing, on a large scale, of special categories of personal data (inter alia sensitive data, biometric data) and personal data relating to criminal convictions and offences.

In cases other than those referred to in points “a” to “c” above, the controller or processor or associations and other bodies representing categories of controllers or processors may designate a DPO. The DPO may act for such associations and other bodies representing controllers or processors.

7.2 What are the sanctions for failing to appoint a Data Protection Officer where required?

The Law does not foresee any sanction for failing to appoint a DPO.

7.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect of his or her role as a Data Protection Officer?

The DPO cannot be dismissed or penalised by the controller or the processor for performing his/her tasks. He/she is bound by secrecy or confidentiality concerning the performance of his/her tasks and shall directly report to the highest management level of the controller or the processor.

7.4 Can a business appoint a single Data Protection Officer to cover multiple entities?

Yes, provided that DPO is easily accessible from each establishment.

7.5 Please describe any specific qualifications for the Data Protection Officer required by law.

The Law provides only for general criteria in this regard. It stipulates only that the DPO shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks assigned to him/her.

Except for the above, the Law does not contain any specific qualifications regarding the DPO.

7.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?

The DPO shall carry out, at least, the following tasks:

a. inform and advise the controller or the processor and the employees who carry out the processing of their obligations pursuant to the Law and to sub-legal acts on data protection;
b. provide advice, where requested, as regards data protection impact assessment, and monitor its performance pursuant to the Law;
c. cooperate with the Agency; and
d. act as the contact point for the Agency on issues relating to processing, including prior consultation on data protection impact assessment; and consult, where appropriate, with regard to any other matter.

7.7 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?

The controller or processor shall publish the contact details of the DPO and communicate them to the Agency.

7.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?

As mentioned in our answer to question 7.7 above, the contact details of the DPO must be published. Except for this requirement, the law does not provide for any specific form dealing with such publication. However, where the personal data are collected from the data subject, the controller shall provide the data subject with all the required information as per the Law, including the contact details of the DPO.
8 Appointment of Processors

8.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?

Yes, the Law establishes that if the processing is conducted by a processor, then the said processing will be governed by a contract/agreement that is binding on the processor with regard to the controller.

8.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?

The agreement must be in writing and shall set out, inter alia, the subject matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects, and the obligations and rights of the controller.

9 Marketing

9.1 Please describe any legislative restrictions on the sending of electronic direct marketing (e.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?).

Controllers may use personal data which they have obtained from publicly accessible sources, or within the framework of the lawful performance of activities, for the purposes of direct marketing through use of mail services, phone calls, email or other telecommunication forms.

However, controllers are obliged to inform the data subjects of their entitlements provided for under the provisions of the law, which include, without limitation, the right of the latter to object to the processing for such direct marketing purposes. If requested by the data subject, the controller is obliged to interrupt the processing permanently or temporarily (as per such request).

In addition to the above, according to the Law no. 04/L-109 on Electronic Communications, the use of automated calling systems without human intervention (automatic calling machines), facsimile machine (fax) or email, for purposes of direct marketing, may be allowed only if the relevant subscribers have given their prior consent.

9.2 Please describe any legislative restrictions on the sending of marketing communications via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.).

Please refer to our answer to question 9.1.

9.3 Do the restrictions noted above apply to marketing sent from other jurisdictions?

As mentioned in our answer to question 3.1 above, the provisions of the Law apply also to data controllers established in another jurisdiction which, for the purpose of personal data processing (in such case, direct marketing), makes use of automatic or other equipment in Kosovo. In such cases, controllers must designate a representative registered in Kosovo.

9.4 Is/are the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?

To the best of our knowledge, the Agency has not been very active in this regard recently.

9.5 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?

The Law does not specifically address this matter; however, if this occurs, the consent of the data subject would be mandatory.

9.6 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?

This is sanctioned by a fine of EUR 10,000. However, if the breach is considered serious and extensive, the maximum fine is EUR 40,000 or, in the case of a company or an enterprise, a fine amounting to between two per cent (2%) and four per cent (4%) of the general turnover of the previous fiscal year, in compliance with the GDPR.

10 Cookies

10.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).

The applicable legislation does not specifically address this matter.

10.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?

Please refer to our answer to question 10.1.

10.3 To date, has/have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?

This is not applicable.

10.4 What are the maximum penalties for breaches of applicable cookie restrictions?

This is not applicable.

11 Restrictions on International Data Transfers

11.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.

Personal data transfers to other jurisdictions may take place only as follows:
a. If the transfer will be made to a jurisdiction with an adequate level of data protection. To this end, the Agency determines and publishes the list of countries pertinent to this group.

b. If authorised by the Agency (in the case of an intended transfer to a country without the adequate level of data protection).

11.2 Please describe the mechanisms businesses typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).

The most common mechanism that businesses typically utilise is the “consent of the data subject” and the “performance of a contract with a data subject”. Only the transfer of personal data to jurisdictions or international organisations without the adequate level of data protection requires prior authorisation from the Agency. The data controller shall provide the Agency with all information necessary regarding the required transfer of personal data; in particular, the categories of data, the purpose of the transfer and the safeguards in place for the protection of personal data in the other country or international organisation. The Agency shall decide on the request without undue delay. However, the respective procedure on obtaining the authorisation for a personal data transfer will be addressed by a sub-legal act of the Agency.

11.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.

12 Whistle-blower Hotlines

12.1 What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?

Law no. 06/L 085 on Protection of Whistle-blowers is the governing legislation. In accordance with this law, current and former employees and/or service providers may report or disclose information which poses a threat or damages the public interest. The following acts and/or omissions of any person are considered to be in the public interest:

a. an offence has been, is being or is likely to be committed;

b. a person has failed, is failing or is likely to fail to comply with any legal obligation;

c. a miscarriage of justice has occurred, is occurring or is likely to occur;

d. the health or safety of any individual has been, is being or is likely to be endangered;

e. the environment has been, is being or is likely to be damaged;

f. a misuse of official duty or authority, public money or resources of a public institution has occurred, is occurring or is likely to occur;

g. an act or omission by or on behalf of a public institution is discriminatory, oppressive, grossly negligent or constitutes serious mismanagement; or

h. information tending to show any matter falling within any of the preceding subparagraphs has been, is being or is likely to be concealed or destroyed.

12.2 Is anonymous reporting prohibited, strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do businesses typically address this issue?

The law on whistle-blowing does not provide for anonymous reporting. According to this law, the official responsible for handling whistle-blowing shall set up a register of the received report and record the following information:

a. the date of receipt;

b. the name and surname of the whistle-blower;

c. the whistle-blower’s contact details;

d. the whistle-blower’s institution; and

e. brief information as to the content of the report.

This law was enacted recently. Hence, so far, we are not aware of any cases of anonymous reporting having been tested in practice.

13 CCTV

13.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?

The Law does not provide specifically for separate registration/notification to, or prior approval from, the Agency regarding the use of CCTV. However, public or private sector persons intending to install video surveillance systems must set up a notice to that effect. Such a notice must be plainly visible and made public in a way that data subjects can easily acquaint themselves with the measures, at the latest, when the video surveillance begins.

13.2 Are there limits on the purposes for which CCTV data may be used?

According to the provisions of the Law, the data collected from video surveillance may be processed or used, if necessary, to achieve the intended purposes and if there are no indications of the violation of legitimate interests of the data subject. These data may be processed or used for other purposes only if this is necessary to prevent threats against the state and public security, or to prosecute crimes.

14 Employee Monitoring

14.1 What types of employee monitoring are permitted (if any), and in what circumstances?

The Law addresses only the video surveillance system in the workplace, which is permitted only in cases where this is necessarily required for the safety of people, security of property and the protection of confidential information, and only if these purposes cannot be achieved by milder means. Video surveillance outside the workplace, particularly in changing rooms, lifts and sanitary areas, and in working areas where there is the potential to infringe the privacy of the employees, is strictly prohibited. The Law is silent on other types of employee monitoring.
14.2 Is consent or notice required? Describe how employers typically obtain consent or provide notice.

Prior to the installation of video surveillance systems in the workplace, the employer must inform the data subjects in writing about their rights and the reasons for the surveillance. The areas monitored must be indicated by the employers through appropriate signs. Consent of the employees is not required.

14.3 To what extent does the works council/employee representatives need to be notified or consulted?

The employer shall inform the trade union representatives, if there are any in place.

15 Data Security and Data Breach

15.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?

The Law requires the processing of personal data to take place in a manner that ensures the security thereof, including protection against unauthorised or unlawful processing, accidental loss, destruction or damage, using appropriate technical or organisational measures.

Therefore, taking into account, inter alia, the state of the art, the costs of implementation and the nature, scope, context and purposes of processing, both the controller and the processor shall implement the appropriate technical and organisational measures in order to ensure a level of security appropriate to the risk.

Such organisational measures may include, without limitation, the following:

a. the pseudonymisation encryption of personal data;
b. the ability to ensure the ongoing confidentiality, integrity and resilience of processing systems and services;
c. the ability to restore availability and access to data in a timely manner in the event of a physical or technical incident; and
d. a process for regularly testing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

15.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

The controller must, without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the Agency of the personal data breach, unless such breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where notification to the Agency is not made within this period, it shall be accompanied by reasons for the delay.

The processor must notify any data breach to the controller without undue delay.

The notification to the Agency shall contain, at least:

a. a description of the nature of the personal data breach, including the categories and approximate number of data subjects concerned, and the categories and approximate number of personal data records concerned;
b. the name and contact details of the DPO or other contact point where more information can be obtained;
c. a description of the likely consequences of the personal data breach; and
d. a description of the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

15.3 Is there a legal requirement to report data breaches to affected data subjects? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

The controller shall communicate the personal data breach to the data subject without undue delay, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons.

The communication to the data subject shall describe, in clear and plain language, the nature of the personal data breach, and contain at least the information indicated in points “b” to “d” of our answer to question 15.2 above.

15.4 What are the maximum penalties for data security breaches?

The maximum penalty for a data security breach is EUR 40,000, or a fine amounting to 2–4% of the annual turnover of the preceding financial year, in compliance with the GDPR.

16 Enforcement and Sanctions

16.1 Describe the enforcement powers of the data protection authority(ies).

<table>
<thead>
<tr>
<th>Investigatory Power</th>
<th>Civil/Administrative Sanction</th>
<th>Criminal Sanction</th>
</tr>
</thead>
</table>
| The Agency may carry out inspections and audits on its own initiative to monitor compliance with data protection rules. | The inspector of the Agency is entitled, inter alia, to:
| a. order the elimination of any irregularities or deficiencies observed, in the manner and within the term set out previously by the latter. This may include the erasure, blocking, destruction, deletion or anonymisation of data in compliance with the Law;
b. impose a temporary ban on the processing of personal data by controllers and processors in the public or private sector who have failed to implement the necessary measures and procedures to secure personal data; | Not applicable. |
c. impose a temporary ban on the processing of personal data, their anonymity, classification and blocking whenever he/she concludes that the personal data are being processed in breach of the legal provisions; | |

16.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?

Concerning the entitlement to impose a ban, please refer to our answer to question 16.1 above.

There is no need for a court order to impose a ban.

16.3 Describe the data protection authority’s approach to exercising those powers, with examples of recent cases.

Please refer to our answer to question 18.1 below.

16.4 Does the data protection authority ever exercise its powers against businesses established in other jurisdictions? If so, how is this enforced?

To the best of our knowledge, it does not.
Ardian Rexha is a Senior Legal Associate in the Tax & Legal Department of Deloitte Kosova Shpk. Ardian holds a Bachelor’s Degree in Law from the University of Pristina, Faculty of Law, and an advanced Master’s Degree in International and European Economic Law (LL.M.) from Maastricht University, Faculty of Law.

Ardian has successfully passed the Bar Exam and prior to joining Deloitte, he worked as a Legal Associate at a law firm and as a Senior Legal Researcher at the Kosovo Judicial Council.

Ardian has more than five years of experience in corporate law, project and corporate finance, mergers and acquisitions, competition, employment, property, consumer and data protection law, among other areas.

Ardian is fluent in Albanian (native speaker) and English. He also has basic knowledge of German and Serbian.

Emirjon Marku
Deloitte Legal Shpk
Rr. Elbasanit, Pallati nr.1
Poshte F. Gjeologji Miniera
Tirana, 1001
Albania
Tel: +355 4451 7920
Email: emarku@deloittece.com
URL: www2.deloitte.com/al/en

Emirjon is a Senior Associate at Deloitte Legal Shpk in Albania. He joined our practice in 2015 from a leading law firm in Albania. Emirjon has more than seven years of experience in corporate law, project and corporate finance, employment, concessions, consumer and data protection law (in Albania and Kosovo), banking, energy, among others. He is an author of several papers and chapters in international legal publications such as the International Comparative Legal Guide series and International Law Office. Emirjon holds a degree in Law from the University of Tirana, Albania (2007), and a Master’s degree in European Law (Eur. LL.M.) from Julius Maximilian University of Würzburg, Germany (2010). He is a member of the Albanian Bar Association.

Emirjon is fluent in Albanian (native speaker), English and German.
Chapter 28

Luxembourg

1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

Since 25 May 2018, the principal data protection legislation in the EU has been Regulation (EU) 2016/679 (the “General Data Protection Regulation” or “GDPR”). The GDPR repealed Directive 95/46/EC (the “Data Protection Directive”) and has led to increased (though not total) harmonisation of data protection law across the EU Member States.

At the national level, the Act of 1 August 2018 on the organisation of the National Data Protection Commission and the general data protection framework (the “Act of 1 August 2018”) completes the GDPR and repeals the previous principal national legislation on data protection (the Act of 2 August 2002 on the protection of personal data, the “Act of 2002”).

Another significant piece of data protection legislation was adopted on the same day as the Act of 1 August 2018: the Act of 1 August 2018 on the protection of personal data with regard to the processing of personal data in criminal and national security matters (the “Act of 1 August 2018 bis”).

1.2 Is there any other general legislation that impacts data protection?

The amended Act of 30 May 2005 concerning the specific provisions for protection of the individual in respect of the processing of personal data in the electronic communications sector (the “Act of 30 May 2005”) transposes European Directive 2002/58/EC into national legislation. It governs the protection of personal data in the field of telecommunications and electronic communications, and takes into account recent and foreseeable developments in the field of services and technologies involving electronic communications.

In January 2017, the European Commission published a proposal for an ePrivacy regulation (the “ePrivacy Regulation”) that would harmonise the applicable rules across the EU. In September 2018, the Council of the European Union published proposed revisions to the draft. The ePrivacy Regulation is still a draft at this stage and it is unclear when it will be finalised.

1.3 Is there any sector-specific legislation that impacts data protection?

There exist sector-specific laws that have a significant impact on data protection in Luxembourg (please note that the following list is not exhaustive):

- **Passenger name records**: The Act of 1 August 2018 on the processing of passenger name record data in the context of the prevention and repression of terrorism and serious crime and amending the Act of 5 July 2016 on the reorganisation of the State Intelligence Service.
- **Patient records**: The Act of 24 July 2014 on the rights and obligations of the patient, as amended by the Act of 8 March 2018 on hospitals and hospital planning.
- **Criminal records**: The Act of 29 March 2013 concerning the organisation of the criminal record and the exchange of information from the criminal record between Member States of the European Union, as amended by the Act of 1 August 2018 bis.
- **Employee monitoring**: Article L. 261-1 of the Luxembourg Labour Code, as amended by Article 71 of the Act of 1 August 2018.

1.4 What authority(ies) are responsible for data protection?

Pursuant to the Act of 1 August 2018, the Luxembourg Supervisory Authority responsible for data protection is the National Commission for Data Protection (the “CNPD”).

2 Definitions

2.1 Please provide the key definitions used in the relevant legislation:

- **“Personal Data”** means any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
- **“Processing”** means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Territorial Scope

3.1 Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to those laws?

The GDPR applies to businesses that are established in any EU Member State, and that process personal data (either as a controller or processor, and regardless of whether or not the processing takes place in the EU) in the context of that establishment.

A business that is not established in any Member State, but is subject to the laws of a Member State by virtue of public international law, is also subject to the GDPR.

The GDPR applies to businesses outside the EU if they (either as controller or processor) process the personal data of EU residents in relation to: (i) the offering of goods or services (whether or not in return for payment) to EU residents; or (ii) the monitoring of the behaviour of EU residents (to the extent such behaviour takes place in the EU).

Further, the GDPR applies to businesses established outside the EU if they monitor the behaviour of EU residents (to the extent such behaviour takes place in the EU).

Key Principles

4.1 What are the key principles that apply to the processing of personal data?

- **Transparency**
  Personal data must be processed lawfully, fairly and in a transparent manner. Controllers must provide certain minimum information to data subjects regarding the collection and further processing of their personal data. Such information must be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

- **Lawful basis for processing**
  Processing of personal data is lawful only if, and to the extent that, it is permitted under EU data protection law. The GDPR provides an exhaustive list of legal bases on which personal data may be processed, of which the following are the most relevant for businesses: (i) prior, freely given, specific, informed and unambiguous consent of the data subject; (ii) contractual necessity (i.e., the processing is necessary for the performance of a contract to which the data subject is a party, or for the purposes of pre-contractual measures taken at the data subject’s request); (iii) compliance with legal obligations (i.e., the controller has a legal obligation, under the laws of the EU or an EU Member State, to perform the relevant processing); or (iv) legitimate interests (i.e., the processing is necessary for the purposes of legitimate interests pursued by the controller, except where the controller’s interests are overridden by the interests, fundamental rights or freedoms of the affected data subjects).

Please note that businesses require stronger grounds to process sensitive personal data. The processing of sensitive personal data is only permitted under certain conditions, of which the most relevant for businesses are: (i) explicit consent of the affected data subject; (ii) the processing is necessary in the context of employment law; or (iii) the processing is necessary for the establishment, exercise or defence of legal claims.

- **Purpose limitation**
  Personal data may only be collected for specified, explicit and legitimate purposes and must not be further processed in a manner that is incompatible with those purposes. If a controller wishes to use the relevant personal data in a manner that is incompatible with the purposes for which they were initially collected, it must: (i) inform the data subject of such new processing; and (ii) must be able to rely on a lawful basis as set out above.

- **Data minimisation**
  Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which those data are processed. A business should only process the personal data that it actually needs to process in order to achieve its processing purposes.

- **Accuracy**
  Personal data must be accurate and, where necessary, kept up to date. A business must take every reasonable step to ensure that personal data that are inaccurate are either erased or rectified without delay.

- **Retention**
  Personal data must be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

- **Data security**
  Personal data must be processed in a manner that ensures appropriate security of those data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

- **Accountability**
  The controller is responsible for, and must be able to demonstrate, compliance with the data protection principles set out above.

Individual Rights

5.1 What are the key rights that individuals have in relation to the processing of their personal data?

- **Right of access to data/copies of data**
  A data subject has the right to obtain from a controller the following information in respect of the data subject’s personal data: (i) confirmation of whether, and where, the
controller is processing the data subject’s personal data; (ii) information about the purposes of the processing; (iii) information about the categories of data being processed; (iv) information about the categories of recipients with whom the data may be shared; (v) information about the period for which the data will be stored (or the criteria used to be determine that period); (vi) information about the existence of the rights to erasure, to rectification, to restriction of processing and to object to processing; (vii) information about the existence of the right to complain to the relevant data protection authority; (viii) where the data were not collected from the data subject, information as to the source of the data; and (ix) information about the existence of, and an explanation of the logic involved in, any automated processing that has a significant effect on the data subject.

Additionally, the data subject may request a copy of the personal data being processed.

- **Right to rectification of errors**
  Controllers must ensure that inaccurate or incomplete data are erased or rectified. Data subjects have the right to rectification of inaccurate personal data.

- **Right to deletion/right to be forgotten**
  Data subjects have the right to erasure of their personal data (the “right to be forgotten”) if: (i) the data are no longer needed for their original purpose (and no new lawful purpose exists); (ii) the lawful basis for the processing is the data subject’s consent, the data subject withdraws that consent, and no other lawful ground exists; (iii) the data subject exercises the right to object, and the controller has no overriding grounds for continuing the processing; (iv) the data have been processed unlawfully; or (v) erasure is necessary for compliance with EU law or national data protection law.

- **Right to object to processing**
  Data subjects have the right to object, on grounds relating to their particular situation, to the processing of personal data where the basis for that processing is either public interest or legitimate interest of the controller. The controller must cease such processing unless it demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the relevant data subject or requires the data in order to establish, exercise or defend legal rights.

- **Right to restrict processing**
  Data subjects have the right to restrict the processing of personal data, which means that the data may only be held by the controller, and may only be used for limited purposes if: (i) the accuracy of the data is contested (and only for as long as it takes to verify that accuracy); (ii) the processing is unlawful and the data subject requests restriction (as opposed to exercising the right to erasure); (iii) the controller no longer needs the data for their original purpose, but the data are still required by the controller to establish, exercise or defend legal rights; or (iv) verification of overriding grounds is pending, in the context of an erasure request.

- **Right to data portability**
  Data subjects have a right to receive a copy of their personal data in a commonly used machine-readable format, and transfer their personal data from one controller to another or have the data transmitted directly between controllers.

- **Right to withdraw consent**
  A data subject has the right to withdraw their consent at any time. The withdrawal of consent does not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject must be informed of the right to withdraw consent. It must be as easy to withdraw consent as to give it.

### 6 Registration Formalities and Prior Approval

<table>
<thead>
<tr>
<th>6.1</th>
<th>Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>There is no general prior notification requirement. Indeed, such kind of notification requirement referred to in the Act of 2002 was abolished by the entry into force of the GDPR and the Act of 1 August 2018.</td>
</tr>
</tbody>
</table>

This is not applicable in our jurisdiction.

<table>
<thead>
<tr>
<th>6.2</th>
<th>If such registration/notice is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>This is not applicable in our jurisdiction.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>6.3</th>
<th>On what basis are registrations/notifications made (e.g., per legal entity, per processing purpose, per data category, per system or database)?</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>This is not applicable in our jurisdiction.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>6.4</th>
<th>Who must register with/notify the data protection authority (e.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation)?</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>This is not applicable in our jurisdiction.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>6.5</th>
<th>What information must be included in the registration/notice (e.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes)?</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>This is not applicable in our jurisdiction.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>6.6</th>
<th>What are the sanctions for failure to register/notify where required?</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>This is not applicable in our jurisdiction.</td>
</tr>
</tbody>
</table>
6.7 What is the fee per registration/notification (if applicable)?

This is not applicable in our jurisdiction.

6.8 How frequently must registrations/notifications be renewed (if applicable)?

This is not applicable in our jurisdiction.

6.9 Is any prior approval required from the data protection regulator?

Where a DPIA (Data Protection Impact Assessment) reveals that an intended processing activity would result in a high risk to the rights and freedoms of natural persons and in the absence of measures taken by the controller to mitigate the risk, the controller shall, prior to the intended processing, consult the Supervisory Authority. The Supervisory Authority will then give an opinion on the planned processing operation and the risk management of the controller. The intended processing may only be carried out after implementing the Supervisory Authority’s recommendations. In addition, according to Article 46(3) of the GDPR, prior approval of the Supervisory Authority is required for transfers of personal data to any third country not offering adequate protection and that are based upon ad hoc contractual clauses rather than the appropriate safeguards referred to in Article 46(2) of the GDPR, e.g. Standard Contractual Clauses approved by the EU Commission.

6.10 Can the registration/notification be completed online?

With regard to the prior consultation referred to in question 6.9, a standard form to be completed is available on the CNPD website.

6.11 Is there a publicly available list of completed registrations/notifications?

This is not applicable in our jurisdiction.

6.12 How long does a typical registration/notification process take?

This is not applicable in our jurisdiction.

7 Appointment of a Data Protection Officer

7.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.

The appointment of a Data Protection Officer for controllers or processors is only mandatory in some circumstances, including where there is: (i) large-scale regular and systematic monitoring of individuals; or (ii) large-scale processing of sensitive personal data. Where a business designates a Data Protection Officer voluntarily, the requirements of the GDPR apply as though the appointment were mandatory.

7.2 What are the sanctions for failing to appoint a Data Protection Officer where required?

In the circumstances where appointment of a Data Protection Officer is mandatory, failure to comply may result in the wide range of penalties available under the GDPR, including administrative fines up to EUR 10,000,000 or, in the case of a company, up to 2% of the previous year’s total annual worldwide turnover, whichever is higher.

7.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect of his or her role as a Data Protection Officer?

The appointed Data Protection Officer should not be dismissed or penalised for performing their tasks and should report directly to the highest management level of the controller or processor.

7.4 Can a business appoint a single Data Protection Officer to cover multiple entities?

A single Data Protection Officer is permitted by a group of undertakings provided that the Data Protection Officer is easily accessible from each establishment.

7.5 Please describe any specific qualifications for the Data Protection Officer required by law.

The Data Protection Officer should be appointed on the basis of professional qualities and should have an expert knowledge of data protection law and practices. While this is not strictly defined, it is clear that the level of expertise required will depend on the circumstances. For example, the involvement of large volumes of sensitive personal data will require a higher level of knowledge.

7.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?

A Data Protection Officer should be involved in all issues which relate to the protection of personal data. The GDPR outlines the minimum tasks required by the Data Protection Officer, which include: (i) informing the controller, processor and their relevant employees who process data of their obligations under the GDPR; (ii) monitoring compliance with the GDPR, national data protection legislation and internal policies in relation to the processing of personal data including internal audits; (iii) advising on data protection impact assessments and the training of staff; and (iv) co-operating with the data protection authority and acting as the authority’s primary contact point for issues related to data processing.

7.7 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?

Yes, the controller or processor must notify the data protection authority of the contact details of the designated Data Protection Officer. In this regard, a standard form to be completed is available on the CNPD website.
7.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?

The Data Protection Officer does not necessarily need to be named in the public-facing privacy notice. However, the contact details of the Data Protection Officer must be notified to the data subject when personal data relating to that data subject are collected whether directly or indirectly. As a matter of good practice, the Article 29 Working Party (the “WP29”) now recommends that both the data protection authority and employees be notified of the name and contact details of the Data Protection Officer.

8 Appointment of Processors

8.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?

Yes. The business that appoints a processor to process personal data on its behalf, is required to enter into an agreement with the processor which sets out – inter alia – the subject matter for processing, the duration of processing, the nature and purpose of processing, the types of personal data and categories of data subjects, and the obligations and rights of the controller (i.e., the business).

It is essential that the processor appointed by the business complies with the GDPR.

8.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?

The processor must be appointed under a binding agreement in writing. The contractual terms must stipulate that the processor: (i) only acts on the documented instructions of the controller; (ii) imposes confidentiality obligations on all employees; (iii) ensures the security of personal data that it processes; (iv) abides by the rules of regarding the appointment of sub-processors; (v) implements measures to assist the controller with guaranteeing the rights of data subjects; (vi) assists the controller in obtaining approval from the relevant data protection authority; (vii) either returns or destroys the personal data at the end of the relationship (except as required by EU or Member State law); and (viii) provides the controller with all information necessary to demonstrate compliance with the GDPR and allows for and contributes to audits, including inspections, conducted by the controller or another auditor mandated by the controller.

9 Marketing

9.1 Please describe any legislative restrictions on the sending of electronic direct marketing (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.).

Pursuant to the Act of 30 May 2005, the use of automated calling and communication systems without human intervention (automatic calling machines), facsimile machines (fax) or electronic mail for the purposes of direct marketing may be allowed only in respect of data subjects who have given their prior consent. No opt-out register must be checked in advance.

9.2 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.).

Pursuant to the Act of 30 May 2005, the use of automated calling and communication systems without human intervention (automatic calling machines), facsimile machines (fax) or electronic mail for the purposes of direct marketing may be allowed only in respect of data subjects who have given their prior consent. No opt-out register must be checked in advance.

9.3 Do the restrictions noted above apply to marketing sent from other jurisdictions?

There is no treaty or other agreement between Luxembourg and third countries on this subject. As far as the EU countries that have transposed the ePrivacy Directive are concerned, it is undeniable that the restrictions apply.

With regard to data controllers established outside the EU, they must comply with the GDPR when they process the personal data of EU residents in relation to the offering of goods or services, whether or not in return for payment (see section 3).

9.4 Is/are the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?

Pursuant to Article 12 of the Act of 30 May 2005, the CNPD is responsible for the application of the provisions of the Act of 30 May 2005.

9.5 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?

Yes, such practice is not prohibited as long as the data protection requirements are respected. It is therefore necessary to ensure, before purchasing such a list, that the personal data appearing on it comply with the requirements of both the GDPR and the Act of 30 May 2005.

9.6 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?

Pursuant to the Act of 30 May 2005, any person who sends marketing communications in breach of applicable restrictions shall be liable to a term of imprisonment lasting between eight days and one year and/or a fine of between EUR 251 and 125,000. In addition, the Court to which the matter is referred may order the cessation of any processing.
10 Cookies

10.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).

The Act of 30 May 2005 implements Article 5 of the ePrivacy Directive. Pursuant to Article 5 of the EU ePrivacy Directive, the storage of cookies (or other data) on an end user’s device requires prior consent (the applicable standard of consent is derived from the GDPR). For consent to be valid, it must be informed, specific, freely given and must constitute a real and unambiguous indication of the individual’s wishes. This does not apply if: (i) the cookie is for the sole purpose of carrying out the transmission of a communication over an electronic communications network; or (ii) the cookie is strictly necessary to provide an “information society service” (e.g., a service over the internet) requested by the subscriber or user, which means that it must be essential to fulfil their request. The controller must also freely give the opportunity to the data subjects to withdraw their consent at any time.

The EU Commission intends to pass a new ePrivacy Regulation that will replace the respective national legislation in the EU Member States. The ePrivacy Regulation is planned to come into force in 2019.

10.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?

As it stands, the applicable legislation does not expressly distinguish between different types of cookies.

10.3 To date, has/have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?

At the present time, the CNPD has not published any guidance on the use of cookies and has not initiated any enforcement action in relation to cookies.

10.4 What are the maximum penalties for breaches of applicable cookie restrictions?

Pursuant to the Act of 30 May 2005, the maximum penalties for breaches of applicable cookie restrictions are a fine of EUR 125,000 and/or imprisonment for eight days.

11 Restrictions on International Data Transfers

11.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.

Data transfers to other jurisdictions that are not within the European Economic Area (the “EEA”) can only take place if the transfer is to an “Adequate Jurisdiction” (as specified by the EU Commission), the business has implemented one of the required safeguards as specified by the GDPR, or one of the derogations specified in the GDPR applies to the relevant transfer. The EDPB Guidelines (2/2018) set out that a “layered approach” should be taken with respect to these transfer mechanisms. If the transfer is not to an Adequate Jurisdiction, the data exporter should first explore the possibility of implementing one of the safeguards provided for in the GDPR before relying on a derogation.

11.2 Please describe the mechanisms businesses typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).

When transferring personal data to a country other than an Adequate Jurisdiction, businesses must ensure that there are appropriate safeguards on the data transfer, as prescribed by the GDPR. The GDPR offers a number of ways to ensure compliance for international data transfers, of which one is consent of the relevant data subject. Other common options are the use of Standard Contractual Clauses or Binding Corporate Rules (“BCRs”).

Businesses can adopt the Standard Contractual Clauses drafted by the EU Commission – these are available for transfers between controllers, and transfers between a controller (as exporter) and a processor (as importer). International data transfers may also take place on the basis of contracts agreed between the data exporter and data importer, provided that they conform to the protections outlined in the GDPR, and they have the prior approval of the relevant data protection authority.

International data transfers within a group of businesses can be safeguarded by the implementation of BCRs. The BCRs will always need approval from the relevant data protection authority. Most importantly, the BCRs will need to include a mechanism to ensure they are legally binding and enforced by every member in the group of businesses. Among other things, the BCRs must set out the group structure of the businesses, the proposed data transfers and their purpose, the rights of data subjects, the mechanisms that will be implemented to ensure compliance with the GDPR and the relevant complainant procedures.

Transfer of personal data to the USA is also possible if the data importer has signed up to the EU-US Privacy Shield Framework, which was designed by the US Department of Commerce and the EU Commission to provide businesses in the EU and the US with a mechanism to comply with data protection requirements when transferring personal data from the EU to the US.

11.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.

It is likely that the international data transfer will require prior approval from the relevant data protection authority unless they have already established a GDPR-compliant mechanism, as set out above, for such transfers.

In any case, most of the safeguards outlined in the GDPR will need initial approval from the data protection authority, such as the establishment of BCRs.
Internal whistle-blowing schemes are generally established in pursuance of a concern to implement proper corporate governance principles in the daily functioning of businesses. Whistle-blowing is designed as an additional mechanism for employees to report misconduct internally through a specific channel and supplements a business’ regular information and reporting channels, such as employee representatives, line management, quality-control personnel or internal auditors who are employed precisely to report such misconduct.

The WP29 has limited its Opinion 1/2006 on the application of EU data protection rules on internal whistle-blowing schemes to the fields of accounting, internal accounting controls, auditing matters, the fight against bribery, banking and financial crime. The scope of corporate whistle-blower hotlines, however, does not need to be limited to any particular issues. In Opinion 1/2006 it is recommended that the business responsible for the whistle-blowing scheme should carefully assess whether it might be appropriate to limit the number of persons eligible for reporting alleged misconduct through the whistle-blowing scheme, and whether it might be appropriate to limit the number of persons who may be reported through the scheme, particularly in the light of the seriousness of the alleged offences reported.

Anonymous reporting is not prohibited under EU data protection law; however, it raises problems as regards the essential requirement that personal data should only be collected fairly. In Opinion 1/2006, the WP29 considered that only identified reports should be advertised in order to satisfy this requirement. Businesses should not encourage or advertise the fact that anonymous reports may be made through a whistle-blower scheme.

An individual who intends to report to a whistle-blowing system should be made aware that he/she will not suffer due to his/her action. The whistle-blower, at the time of establishing the first contact with the scheme, should be informed that his/her identity will be kept confidential at all the stages of the process and, in particular, will not be disclosed to third parties, such as the incriminated person or the employee’s line management. If, despite this information, the person reporting to the scheme still wants to remain anonymous, the report will be accepted into the scheme. Whistle-blowers should be informed that their identity may need to be disclosed to the relevant people involved in any further investigation or subsequent judicial proceedings instigated as a result of any inquiry conducted by the whistle-blowing scheme.

There is no strict limitation on the purposes for which CCTV may be used. However, in its 2018 guidelines, the CNPD insists that permanent and continuous monitoring may undermine the principle of data minimisation.

In addition, the CNPD makes it clear that CCTV must not be used to monitor the behaviour and performance of the controller’s employees other than for the purposes for which it was set up.

According to Article 71 of the Act of 1 August 2018, the processing of personal data for the purpose of monitoring employees in the context of employment relations may only be carried out by the employer in the cases referred to in Article 6 (1) a) to f) of the GDPR. This contrasts with the former wording of Article L.261-1 of the Labour Code, which provided for an exhaustive list of specific purposes (e.g. to ensure the security and health of employees, protection of employer’s property, etc.).
Types of employee monitoring:

- **CCTV**: see section 13.
- **Monitoring the use of IT tools**: the employer may only monitor the use of employees’ IT tools for the purpose of protecting the company’s assets. In principle, this is the only criterion on which such monitoring can be legitimised.
- **Recording of telephone conversations**: recordings of telephone conversations at the workplace can only be used as evidence of a commercial transaction or “other” commercial communication, in the event of any disputes. Recordings of private conversations, as well as recordings whose purposes do not fall within the legal provisions, are therefore not allowed.
- **Geolocation devices**: in principle, this kind of processing activity must be subject to a DPIA prior to their implementation.

### 14.2 Is consent or notice required? Describe how employers typically obtain consent or provide notice.

Consent is not required as it would not be freely given, taking into account the imbalance of power existing between the employer and the employee.

Nevertheless, in order to comply with the GDPR, the employer must inform its employees of the different processing activities, including monitoring measures.

A clear and comprehensive privacy policy is a good way to inform employees (see question 13.1 concerning notices indicating the operation of CCTV).

### 14.3 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?

According to the Article L.261-1 of the Labour Code and without prejudice to the data subject’s right to information, the employer shall inform in advance the Joint Committee or, failing that, the staff delegation or, failing that, the labour and mining inspection.

This prior notice shall contain a detailed description of the purposes of the proposed processing activities, the arrangements for implementing the monitoring system and, where applicable, the duration or criteria for storing the data, as well as a formal undertaking by the employer that the data collected will not be used for a purpose other than that explicitly provided for in the prior notice.

### 15 Data Security and Data Breach

#### 15.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?

Yes. Personal data must be processed in a way which ensures security and safeguards against unauthorised or unlawful processing, accidental loss, destruction and damage of the data.

Both controllers and processors must ensure they have appropriate technical and organisational measures to meet the requirements of the GDPR. Depending on the security risk, this may include the encryption of personal data, the ability to ensure the ongoing confidentiality, integrity and resilience of processing systems, an ability to restore access to data following a technical or physical incident, and a process for regularly testing and evaluating the technical and organisational measures for ensuring the security of processing.

#### 15.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

The controller is responsible for reporting a personal data breach without undue delay (and in any case within 72 hours of first becoming aware of the breach) to the relevant data protection authority, unless the breach is unlikely to result in a risk to the rights and freedoms of the data subject(s). A processor must notify any data breach to the controller without undue delay.

The notification must include the nature of the personal data breach, including the categories and number of data subjects concerned, the name and contact details of the Data Protection Officer or relevant point of contact, the likely consequences of the breach and the measures taken to address the breach, including attempts to mitigate possible adverse effects.

#### 15.3 Is there a legal requirement to report data breaches to affected data subjects? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

Controllers have a legal requirement to communicate the breach to the data subject, without undue delay, if the breach is likely to result in a high risk to the rights and freedoms of the data subject.

The notification must include the name and contact details of the Data Protection Officer (or point of contact), the likely consequences of the breach and any measures taken to remedy or mitigate the breach.

The controller may be exempt from notifying the data subject if the risk of harm is remote (e.g., because the affected data is encrypted), the controller has taken measures to minimise the risk of harm (e.g., suspending affected accounts) or the notification requires a disproportionate effort (e.g., public notice of the breach).

#### 15.4 What are the maximum penalties for data security breaches?

The maximum penalty is the higher of €20 million or 4% of worldwide turnover.
16.1 Describe the enforcement powers of the data protection authority(ies).

<table>
<thead>
<tr>
<th>Investigatory Power</th>
<th>Civil/Administrative Sanction</th>
<th>Criminal Sanction</th>
</tr>
</thead>
<tbody>
<tr>
<td>Investigative Powers</td>
<td>The data protection authority has wide powers to order the controller and the processor to provide any information it requires for the performance of its tasks, to conduct investigations in the form of data protection audits, to carry out review on certificates issued pursuant to the GDPR, to notify the controller or processor of alleged infringement of the GDPR, to access all personal data and all information necessary for the performance of controllers’ or processors’ tasks, and to access the premises of the data including any data processing equipment.</td>
<td>N/A</td>
</tr>
<tr>
<td>Corrective Powers</td>
<td>The data protection authority has a wide range of powers including to issue warnings or reprimands for non-compliance, to order the controller to disclose a personal data breach to the data subject, to impose a permanent or temporary ban on processing, to withdraw a certification and to impose an administrative fine (as below).</td>
<td>N/A</td>
</tr>
<tr>
<td>Authorisation and Advisory Powers</td>
<td>The data protection authority has a wide range of powers to advise the controller, accredit certification bodies and to authorise certificates, contractual clauses, administrative arrangements and binding corporate rules as outlined in the GDPR.</td>
<td>N/A</td>
</tr>
<tr>
<td>Imposition of administrative fines for infringements of specified GDPR provisions</td>
<td>The GDPR provides for administrative fines which can be €20 million or up to 4% of the business’s worldwide annual turnover of the preceding financial year.</td>
<td>N/A</td>
</tr>
<tr>
<td>Non-compliance with a data protection authority</td>
<td>The GDPR provides for administrative fines which will be €20 million or up to 4% of the business’s worldwide annual turnover of the preceding financial year, whichever is higher.</td>
<td>N/A</td>
</tr>
</tbody>
</table>

16.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?

The GDPR entitles the relevant data protection authority to impose a temporary or definitive limitation including a ban on processing.

16.3 Describe the data protection authority’s approach to exercising those powers, with examples of recent cases.

To our current knowledge, the CNPD has never exercised this type of power.

16.4 Does the data protection authority ever exercise its powers against businesses established in other jurisdictions? If so, how is this enforced?

To our current knowledge, the CNPD has never exercised its powers against businesses established in other jurisdictions.

17 E-discovery / Disclosure to Foreign Law Enforcement Agencies

17.1 How do businesses typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?

There is no publicly available data on this matter.

17.2 What guidance has/have the data protection authority(ies) issued?

The CNPD has not issued specific guidance on this matter. However, it is worth highlighting that the WP29 issued an opinion in 2009 (working document 1/2009 – WP158) on pre-trial discovery for cross-border civil litigation.

18 Trends and Developments

18.1 What enforcement trends have emerged during the previous 12 months? Describe any relevant case law.

There is no publicly available data on this matter.

18.2 What “hot topics” are currently a focus for the data protection regulator?

- The implementation of the “GDPR-CARPA certification” (Certified Assurance Report Based Activities)
  The GDPR-CARPA certification mechanism is the result of a proactive approach taken by the CNPD in order to provide data controllers and processors access to a flexible and highly professional certification mechanism, compliant with Articles 42 and 43 of the GDPR as well as the related guidance from the Article 29 Working Party.
  The GDPR-CARPA certification was open to public consultation until 29 June 2018 and should therefore be completed in 2019.
- Opinion 26/2018 on the draft list of the competent supervisory authority of Luxembourg regarding the processing operations subject to the requirement of a data protection impact assessment (Article 35(4) GDPR)
  Pursuant to Article 35(4) of the GDPR, the CNPD has drafted a list of processing activities for which a DPIA is mandatory. The draft list has been submitted to the European Data Protection Supervisor (“EDPS”) for an opinion.
  The list published by the CNPD (11 March 2019) takes into account the comments submitted by the EDPS.
A founding partner of thg IP/ICT, Raymond has more than 15 years of experience in the field of legal advice, especially Intellectual Property and ICT-related matters.

He started his career as a lawyer at the Liège Bar (Belgium), then acted as a senior trademark and design attorney in one of the leading IP firms in Europe.

Raymond graduated from the Université catholique de Louvain (Belgium) in 2002 and was an assistant lecturer at the same university’s department for civil procedure law for two years.

Raymond is an EUIPO professional representative, obtained a DPO certificate and holds the IAPP’s CIPP/E and CIPM credentials.

Raymond is also member of various professional associations such as IAPP, APDL and AFCDP.

Languages: German, French and English.

Milan joined the Intellectual Property and Information and Communication Technologies legal practice of thg IP/ICT in 2017. Since then, he has advised clients mainly on privacy and data protection, e-commerce and intellectual property matters.

He obtained a Master’s degree in European Law from the Université catholique de Louvain (Belgium) in 2016. The following year, Milan completed the Advanced Master of Laws programme in information technology and communication law at the University of Namur (Belgium). Within the framework of this one-year Advanced Master’s, he also had the opportunity to take part in the LL.M. in Information and Communication Technology Law at the University of Oslo (Norway). Milan also holds the IAPP’s CIPP/E credential.

Milan is a member of various professional associations such as IAPP, APDL and AFCDP.

Languages: French, English and Spanish.

As a medium-sized firm, thg IP/ICT offers personalised and solution-oriented advice. Our specialists have the relevant knowledge, training and certifications to advise our clients on a large range of complex matters, with a pragmatic and hands-on approach.

In addition, our combined expertise in various areas such as intellectual property, data protection, e-commerce, unfair business practices or consumer protection makes us a competent partner, able to tailor our interventions to the specific needs of our clients.

Being part of the thg network, offering a wide range of business consultancy services, from traditional accounting, tax, advisory and human resources to more specialised advisory services, allows our clients to have access to a broad base of expertise. Global vision, quality and reliability are all part of our DNA.
1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

The main legislation is Law no. 8/2005, of August 22 – Personal Data Protection Act (“Lei da Protecção de Dados Pessoais” in Portuguese, or LPDP) of the Macau Special Administrative Region (henceforth “MSAR”).

1.2 Is there any other general legislation that impacts data protection?

The Chief Executive Dispatch no. 83/2007, of March 12, (and ancillary legislation) created the Office for Personal Data Protection (“Gabinete de Protecção de Dados Pessoais” in Portuguese, or “GPDP”).

1.3 Is there any sector-specific legislation that impacts data protection?

Yes – Law no. 2/2012, of March 19, on the Legal Regime of video surveillance in public spaces (“Regime jurídico da videovigilância em espaços públicos” in Portuguese).

1.4 What authority(ies) are responsible for data protection?

The GPDP is the entity responsible for the monitoring and coordination of compliance with the LPDP, as well as for the establishment of an adequate confidentiality regime and the monitoring of its execution.

2 Definitions

2.1 Please provide the key definitions used in the relevant legislation:

■ “Personal Data”

“Personal Data” is defined as “any information of any kind and regardless of the respective format, pertaining to an identified or identifiable natural person. An identifiable person is one who can be identified, directly or indirectly, namely by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity”.

■ “Processing”

“[Data] Processing” is defined as “any operation or set of operations performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction”.

■ “Controller”

The term “Controller” does not exist as such in the LPDP. The closest definition pertains to the “[entity] responsible for processing”, which is defined as “the natural or legal person, public authority, agency or any other body which alone or jointly with others, determines the purposes and means of the processing of personal data” (henceforth “data controller”).

■ “Processor”

The term “Processor” also does not exist as such in the LPDP. The closest definition pertains to “subcontractor”, which is defined as “a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the data controller” (henceforth “data processor”).

■ “Data Subject”

“Data Subject” is defined as “the individual person to whom the data being processed pertains”.

■ “Sensitive Personal Data”

“Sensitive Personal Data” is referred to in article 7 of the LPDP, which prohibits the processing of personal data concerning political or philosophical beliefs, political or trade-union membership, religious faith, private life, racial or ethnic origin, as well as the processing of data concerning health and sex life, including genetic information, with the exceptions foreseen by the LPDP.

■ “Data Breach”

The term “Data Breach” does not exist as such in the LPDP – however, the law provides for the definition of wrongful or undue access as the unauthorised access to personal data by any entity who is not entitled to do so, and stipulates a penalty of imprisonment of up to one year or a fine of up to 120 days (with the aggravating factors indicated in the law and unless a more severe penalty exists by special law).

Other key definitions – please specify (e.g., “Pseudonymous Data”, “Direct Personal Data”, “Indirect Personal Data”)

Other definitions provided by the LPDP include:

■ “personal data file” (“file”) is defined as “any structured set of personal data which are accessible according to specific
criteria, regardless of the form or type of their creation, storage and organisation”;

- “third party” is defined as “any natural or legal person, public authority, agency or any other body other than the data subject, the data controller, the subcontractor or the persons who, under the direct authority of the data controller or of the subcontractor, are authorised to process the data”;

- “recipient” is defined as “a natural or legal person, public authority, agency or any other body to whom data are disclosed, whether a third party or not; however, authorities which may receive data in the framework of a legal stipulation or of a regulatory requirement of organic nature shall not be regarded as recipients”;

- “data subject’s consent” is defined as “any freely given specific and informed indication of his/her wishes by which the data subject signifies his agreement to personal data relating to him being processed”; and

- “interconnection of data” is defined as “data processing which consists in the possibility of correlating data in a file with the data in a file or files kept by another or other controllers, or kept by the same controller for other purposes”.

3 Territorial Scope

3.1 Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to those laws?

The LPDP only provides a territorial scope for its applicability regarding video surveillance or other means of capturing, processing and disseminating sounds and images to identify persons whenever the controller is domiciled in the MSAR, or uses a computer and telematic network access provider established therein.

Therefore, the LPDP shall apply in accordance to its material scope, i.e. it shall apply to the processing of personal data wholly or partly by automated means, as well as processing by non-automated means of personal data contained in or intended for manual files, regardless of the establishment of businesses in other jurisdictions.

Although the LPDP would de jure be applicable in the above case, the jurisdiction of the GPDP would de facto have implementation difficulties regarding a business established in another jurisdiction and with no presence in Macau.

4 Key Principles

4.1 What are the key principles that apply to the processing of personal data?

- Transparency
  Data processing shall be made in a transparent way and in strict compliance with the respect of privacy (article 2 of the LPDP).

- Lawful basis for processing
  Data shall be processed in a lawful way and in compliance with the principle of good faith, as well as with the principles enunciated in article 2 of the LPDP, which include the respect of rights, freedoms and guarantees in the MSAR, in international instruments and in existing legislation (article 5, paragraph 1, subparagraph 1 of the LPDP).

  Article 6 of the LPDP further provides that the processing of personal data may only be carried out if the data subject has given his/her unequivocal consent, or if the processing is necessary for the:
  1) execution of contracts or contracts in which the data subject is a party or prior to the formation of the contract or declaration of negotiation will be made at his request;
  2) compliance with a legal obligation to which the controller is subject;
  3) protection of vital interests of the data subject, if he/she is physically or legally incapable of giving his/her consent;
  4) execution of a mission of public interest or in the exercise of powers of a public authority in which the controller (or a third party to whom the data are transmitted) is invested; and
  5) pursuit of legitimate interests of the controller or third party to whom the data are transmitted, provided that the interests or rights, freedoms and guarantees of the data subject shall not prevail.

- Purpose limitation
  Data shall be collected for specific, determined and lawful purposes, which are directly related to the activity of the data controller, and cannot subsequently be processed in a way that is incompatible with those purposes (article 5, paragraph 1, subparagraph 2 of the LPDP).

- Data minimisation
  No specific stipulation – this principle is included in article 5, paragraph 1, subparagraph 3 of the LPDP (see “Proportionality” below).

- Proportionality
  Data shall be adequate, pertinent and non-excessive in relation to the purposes for which they are collected and processed (article 5, paragraph 1, subparagraph 3 of the LPDP).

- Retention
  Data shall be kept in a way which allows the identification of their owner only for the duration necessary for the purposes of collection or subsequent processing (article 5, paragraph 1, subparagraph 5 of the LPDP).

- Other key principles – please specify
  The LPDP also stipulates that data shall be exact and, if necessary, shall be updated, with the obligation to ensure that inexact or incomplete data are erased or amended, in compliance with the purposes for which the data were collected or subsequently processed (article 5, paragraph 1, subparagraph 5 of the LPDP).

5 Individual Rights

5.1 What are the key rights that individuals have in relation to the processing of their personal data?

- Right of access to data/copies of data
  The LPDP guarantees the right of the data subject to information regarding the identity of the data controller or its representative, the purposes of processing and other ancillary information (article 10 of the LPDP), as well as the right of access to all his/her data (article 11 of the LPDP).

  No specific provisions exist regarding the right to obtain a copy of the personal data.

- Right to rectification of errors
  The right of access includes the right to rectify, delete or block data whose processing does not comply with the LPDP, namely in regard to the incomplete or inexact character of those data (article 11, paragraph 1, subparagraph 4 of the LPDP).
Right to deletion/right to be forgotten

If such registration/notification is needed, must it be of the GPDP, personal data shall be kept in a way which allows the identification of their owner for the duration necessary for the purposes of collection or subsequent processing (as per the principle of retention above).

Right to object to processing

The data subject has the right to object to any, under lawful and serious reasons relating to his/her specific case, that his/her data be the subject of processing, in which case, under justified objection, the processing shall not concern those data (article 12, paragraph 1 of the LPDP).

Right to restrict processing

Without prejudice to the right to object to the processing indicated above, no specific provisions exist regarding the right to restrict processing of personal data. Hence, as long as the data subject presents lawful and serious reasons relating to his/her specific case, he/she shall have the right to restrict processing.

Right to data portability

No specific provisions exist regarding the right to data portability.

Right to withdraw consent

No specific provisions exist regarding the right to withdraw consent. However, we are of the view that this right falls under the provisions regarding the data subject’s right to object to processing (as indicated above) and, therefore, the data subject may withdraw consent insofar as he/she presents lawful and serious reasons relating to his/her specific case to do so.

Right to object to marketing

The data subject also has the right to object, on request and free of charge, to processing of personal data concerning him/her for direct marketing or any other form of commercial prospecting, and also has the right to be informed in advance of any transfer of data to third parties for the purposes of direct marketing or usage for third parties, as well as the right to object, free of charge, to such transfer or usage (article 12, paragraph 2 of the LPDP).

Right to complain to the relevant data protection authority(ies)

The LPDP provides for the possibility to submit a complaint to the GPDP, without prejudice to the possibility of resorting to administrative or jurisdictional means to guarantee the compliance with legal and regulatory provisions (article 28 of the LPDP).

Other key rights – please specify

The LPDP also includes the right not to be subject to automated individual decisions (article 13 of the LPDP) and the right to an indemnity in cases of illegal processing of data or of any act infringing legal or regulatory provisions regarding data protection (article 14 of the LPDP).

6 Registration Formalities and Prior Approval

6.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?

Any data processing is subject to notification of the GPDP, to be made within eight days of the start of such processing by the data controller or by its representative (article 21, paragraph 1 of the LPDP).

If there is transfer of personal data to a destination outside the MSAR, the opinion of the GPDP must be sought to confirm if such destination ensures an adequate level of protection. However, the transfer of personal data to a legal system which does not ensure an adequate level of protection pursuant to the LPDP may be effected by means of notification to the public authority, if the data subject has given his/her unequivocal consent to the transfer, or if that transfer is necessary under the cases provided by law – i.e. it is necessary for the formation of a contract between the data subject and the data controller, for preliminary measures for the formation of said contract by request of the data subject, among others (article 19, paragraph 1 and article 20, paragraph 1 of the LPDP).

The processing of sensitive data or of data related to credit and solvency of its subjects, the interconnection of personal data and the usage of personal data for purposes which are not decisive to the collection of such data are subject to prior authorisation by the GPDP, without prejudice to legal or regulatory exceptions (article 22 of the LPDP).

6.2 If such registration/notification is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?

Any requests for authorisation, notification or opinion sent to the GPDP shall contain the information provided by law, in particular:

1) name and address of the data controller and, if applicable, its representative;
2) purpose of data processing;
3) description of the categories of data subjects and data or categories of personal data concerning said data subjects;
4) recipients or categories of recipients to whom the data may be disclosed and under which conditions;
5) entity in charge of the processing of data, if not the data controller;
6) possible interconnection of processing of personal data;
7) personal data storage period;
8) form and conditions for data subjects to have knowledge of or to amend their respective personal data;
9) expected data transfers to third countries or territories; and
10) general description enabling a preliminary assessment of the suitability of measures taken to ensure the adequate level of protection under the LPDP (in accordance with articles 15 and 16 of the LPDP).

6.3 On what basis are registrations/notifications made (e.g., per legal entity, per processing purpose, per data category, per system or database)?

As previously indicated, any data processing (see “[data] processing” definition above) is subject to notification of the GPDP, regardless of the entity responsible for the processing, without prejudice to the cases where prior consent of the GPDP must be sought.
6.4 Who must register with/notify the data protection authority (e.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation)?

The data controller or its representative has the obligation to notify the GPDP, as per article 21, paragraph 1 of the LPDP.

6.5 What information must be included in the registration/notification (e.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes)?

Any requests for an opinion or authorisation, as well as notifications, sent to the GPDP shall contain the information indicated in subparagraph 2 above (article 23 of the LPDP).

In case of sensitive data processing (article 7, paragraph 2 of the LPDP), of the creation and maintenance of records regarding suspicions of illegal activities, criminal offences and administrative offences (article 8, paragraph 1 of the LPDP), and of requests for authorisation, as well as those pertaining to records of processing of personal data, these shall indicate, at least:

1) the person responsible for the file and, where appropriate, his representative;
2) the categories of personal data processed;
3) the purposes for which the data are intended and the categories of entities to whom they may be transmitted;
4) how the right of access and of rectification of data can be exercised;
5) possible interconnections of processing of personal data; and
6) expected data transfers to third countries or territories.

6.6 What are the sanctions for failure to register/notify where required?

The lack of notification or authorisation request as provided by the LPDP entails a fine of between 2,000 and 20,000 MOP for individuals and a fine of between 10,000 and 100,000 MOP for legal persons. The fine shall be increased to twice its limits in the case of data subject to prior authorisation (in accordance with article 22 of the LPDP).

6.7 What is the fee per registration/notification (if applicable)?

This is not applicable.

6.8 How frequently must registrations/notifications be renewed (if applicable)?

This is not applicable (without prejudice to the obligation to notify the GPDP regarding any new data processing).

6.9 Is any prior approval required from the data protection regulator?

As indicated above, the processing of sensitive data or of data related to credit and solvency of their subjects, the interconnection of personal data and the usage of personal data for purposes which are not decisive to the collection of such data are subject to prior authorisation by the GPDP, without prejudice to legal or regulatory exceptions (article 22 of the LPDP).

6.10 Can the registration/notification be completed online?

The registration/notification is currently not possible online.

6.11 Is there a publicly available list of completed registrations/notifications?

No such list is available.

6.12 How long does a typical registration/notification process take?

No timeframe currently exists for the procedure of prior approval.

7 Appointment of a Data Protection Officer

7.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.

The appointment of a Data Protection Officer is optional – such possibility is not foreseen by the LPDP.

7.2 What are the sanctions for failing to appoint a Data Protection Officer where required?

This is not applicable.

7.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect of his or her role as a Data Protection Officer?

This is not applicable.

7.4 Can a business appoint a single Data Protection Officer to cover multiple entities?

This is not applicable.

7.5 Please describe any specific qualifications for the Data Protection Officer required by law.

This is not applicable.

7.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?

This is not applicable.

7.7 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?

This is not applicable – however, this information shall be included in the notification to be submitted by the applicant to the GPDP (see above).
7.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?

This is not applicable.

8 Appointment of Processors

8.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?

The LPDP stipulates that, where processing is carried out on the data controller’s behalf, said data controller must choose a processor providing sufficient guarantees in respect of the technical security measures and organisational measures governing the processing to be carried out, and must ensure compliance with those measures. The carrying out of processing by way of a processor must be governed by a contract or legal act binding the processor to the controller and stipulating, in particular, that the processor shall act only on instructions from the controller, and that the obligations incumbent on the data controller shall also be incumbent on the processor, inter alia:

a) The data processor must implement appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

b) The measures indicated above must ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected, according to the state of the art and the cost of their implementation.

8.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?

The carrying out of processing by way of a processor must be governed by a contract or legal act binding the processor to the controller and stipulating, in particular, that the processor shall act only on instructions from the controller, and that the obligations set out in paragraphs a) and b) above shall also be incumbent on the processor. For the purposes of keeping proof, the parties of the contract or the legal act relating to data protection, and the requirements relating to the measures referred to in the previous question, must be in writing, in a document with legally recognised probative value.

9 Marketing

9.1 Please describe any legislative restrictions on the sending of electronic direct marketing (e.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?).

As indicated above, data shall be collected for specific, determined and lawful purposes, which are directly related to the activity of the data controller, and cannot subsequently be processed in a way that is incompatible with those purposes (article 5, paragraph 1, subparagraph 2 of the LPDP).

Also, as stated in question 4.1 above, the processing of personal data may only be carried out if the data subject has given his/her unequivocal consent, or if the processing is necessary to the cases referred to in article 6 of the LPDP.

Hence, if the processor has declared marketing communications (be it via electronic direct marketing or via other means) as one of the purposes of processing, and if the data subject has given his/her consent to such purpose, such processing is lawful under the LPDP.

9.2 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.).

Please see question 9.1 above.

9.3 Do the restrictions noted above apply to marketing sent from other jurisdictions?

Please see question 9.1 above. Also, regarding certain industries (e.g. banking and financial industries), the sending of marketing is specifically forbidden to prospective clients without the entity being duly licensed in the MSAR.

9.4 Is/are the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?

Please note that, to the best of our knowledge, such data is not publicly available.

9.5 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?

No specific provisions exist regarding such purchase, although said purchase might constitute an unlawful transfer of personal data if proper consent from the data subject has not been sought.

9.6 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?

If the measures indicated in question 9.1 have not been taken, the entity responsible for treatment is liable to an administrative offence, punishable with a fine of between 8,000 and 80,000 MOP, for non-compliance with the obligations under article 6 of the LPDP (article 33 of the LPDP).

10 Cookies

10.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).

The LPDP does not specifically provide for the use of cookies – hence, opt-in consent must be sought from the data subject.
10.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?

This is not applicable.

10.3 To date, has/have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?

This is not applicable.

10.4 What are the maximum penalties for breaches of applicable cookie restrictions?

This is not applicable.

11 Restrictions on International Data Transfers

11.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.

The transfer of personal data abroad can only take place under the stipulations of the LPDP and only if the legal order to which data are transferred ensures an adequate level of protection. Such level of protection is assessed by the GPDP on a case-by-case basis (article 19 of the LPDP).

11.2 Please describe the mechanisms businesses typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).

The transfer of data abroad may be possible under the exceptions provided by the LPDP, which include the need of such transfer for the formation of a contract between the data subject and the data controller, and for preliminary measures for the formation of said contract by request of the data subject, among others.

However, the most common exception to the rule indicated above is the obtaining of the data subject’s unequivocal consent to the transfer (article 20, paragraph 1 of the LPDP).

11.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.

As no list of legal orders ensuring an adequate level of protection currently exists, the transfer of personal data abroad is subject to prior authorisation by the GPDP, as indicated above. If unequivocal consent of the data subject is obtained, or if the situation under analysis falls under one of the exceptions provided by the LPDP, a simple notification is enough.

No timeframe currently exists for the procedure of assessment of the level of protection of a given legal order by the GPDP.

12 Whistle-blower Hotlines

12.1 What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?

No provisions exist in the LPDP regarding whistle-blower hotlines; neither is any binding guidance issued by the GPDP. As indicated in question 5.1 above, the LPDP provides for the possibility to submit a complaint to the GPDP, without prejudice to the possibility of resorting to administrative or jurisdictional means to guarantee compliance with legal and regulatory provisions (article 28 of the LPDP).

12.2 Is anonymous reporting prohibited, strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do businesses typically address this issue?

No provisions exist in the LPDP regarding this issue and, to the best of our knowledge, there is no binding guidance on this matter.

13 CCTV

13.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?

The LPDP applies to video surveillance and to other means of capturing, processing and disseminating sounds and images to identify persons, whenever the controller is domiciled or headquartered in the MSAR, or uses a provider of access to computer and telematic networks established there (article 3, paragraph 3 of the LPDP).

No other specific stipulations exist for video surveillance, with the exception of Law no. 2/2012, of March 19, which establishes the legal framework of video surveillance in public spaces by the security forces and services of the MSAR.

As the use of CCTV is a separate processing of data, it shall require a separate notification to the GPDP under the law.

13.2 Are there limits on the purposes for which CCTV data may be used?

In accordance with GPDP guidelines, and without prejudice to the principles of purpose limitation and proportionality set out in the question above, data controllers shall obey the following rules regarding CCTV in order not to violate the PDPA regime, as well as other stipulations contained in other legislation such as the Macau Penal Code:

- Only images can be recorded, not sound.
- The camera cannot be hidden and its existence must be publicised.
- The system cannot be connected to a public network (for instance, Wi-Fi networks or remote control functions).
- The areas covered by the footage should not be excessive, i.e. they should not include neighbouring areas.
- Security must be the exclusive purpose of data collection.
Third parties cannot have access to the data, except when allowed by law.
- It is forbidden to replay recorded footage.
- The data can only be preserved for six months.

14 Employee Monitoring

14.1 What types of employee monitoring are permitted (if any), and in what circumstances?

Without prejudice to the data which shall be mandatorily collected by the employer under the Macau Labour Law, no specific provision exists on this matter. Therefore, employee monitoring is possible if it is necessary under the cases provided by the LPDP, or if consent has been sought.

14.2 Is consent or notice required? Describe how employers typically obtain consent or provide notice.

Under the LPDP, the processing of data can only take place if the data subject has given his/her unequivocal consent to the transfer, or if that transfer is necessary under the cases provided by law (see “Key Principles” above).

As indicated above, the LPDP also allows for the processing of data if such processing is necessary for pursuing legitimate interests of the data controller or third party to whom the data are communicated, insofar as the interests or rights, freedoms and guarantees of the data subject do not prevail.

In the case of employee monitoring, the usual procedure to obtain consent would be to prepare an appropriate declaration of consent describing the applicable rules and rights of the data subject/employee under the LPDP.

14.3 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?

No specific provisions exist on this matter.

15 Data Security and Data Breach

15.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?

Yes – in accordance with the LPDP, the data controller shall implement appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction, accidental loss, unauthorised disclosure or access, \textit{inter alia}, when processing involves transmission over a network, and against any form of unlawful processing, having regard to the available technical knowledge and to the costs resulting from its implementation, an adequate level of security with regard to the risks involved with the processing and the nature of the data to be protected (article 15, paragraph 1 of the LPDP).

The LPDP also provides for special security measures in case of sensitive data processing and of the creation and maintenance of records regarding suspicions of illegal activities, criminal offences and administrative offences (article 7, paragraph 2, article 8, paragraph 1 and article 16, paragraph 1 of the LPDP), namely appropriate measures to:

- prevent unauthorised access to the premises used for the processing of such data (control of entry to the premises);
- prevent data carriers from being read, copied, altered or removed by an unauthorised person (control of data carriers);
- prevent unauthorised entry, as well as unauthorised disclosure, alteration or deletion of inserted personal data (insertion control);
- prevent automated data processing systems from being used by unauthorised persons through data transmission facilities (monitoring of use);
- ensure that authorised persons can only access the data covered by the authorisation (access control);
- ensure the verification of entities to whom personal data may be transmitted through data transmission facilities (transmission control);
- ensure that there is \textit{a posteriori} verification, within a period appropriate to the nature of the processing, to be laid down in the rules applicable to each sector, of the personal data to be introduced, when and by whom (introduction control); and
- prevent the data from being read, copied, altered or disposed of in an unauthorised manner during the transmission of personal data and in the transport of its medium (transport control).

Also, the LPDP requires that the systems must ensure the logical separation of data on health and sexual life, including genetic data, from other personal data (article 16, paragraphs 1 and 3 of the LPDP).

In case of sensitive data indicated in article 7 of the LPDP, the GPDP may require the encryption of data for transmissions over a network, if said transmission may imperil rights, freedoms and guarantees of the data subjects (article 16, paragraph 4 of the LPDP).

15.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

No specific provision exists on this matter.

15.3 Is there a legal requirement to report data breaches to affected data subjects? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

Without prejudice to the right of information, which may be exercised by the data subject, no specific provision exists on this matter.

15.4 What are the maximum penalties for data security breaches?

Non-compliance with the special security measures for sensitive data processing and for the creation and maintenance of records regarding suspicions of illegal activities, criminal offences and administrative offences, set out in article 16 of the LPDP and described in question 15.1 above, is an administrative offence which may entail a fine between 4,000 and 40,000 MOP.
Although the LPDP provides penalties for undue access, as well as for tampering or the destruction of personal data, it does not specifically provide for security breaches by the data controller. It should be noted, however, that the LPDP mandates that the data controller shall present the notification/authorisation request with a general description of the security measures indicated in question 15.1 above, so that the GPDP may evaluate the adequacy of such measures. If the GPDP notifies the above-mentioned entity to address any insufficiency in the security measures and no remedy is taken, then a fine of between 2,000 and 20,000 MOP for individuals and a fine of between 10,000 and 100,000 MOP for legal persons may be imposed.

In case of wrongful or undue access to personal data by any entity who is not entitled to do so, the LPDP stipulates, as a maximum penalty, two years of imprisonment or a fine of up to 240 days (unless a more severe penalty exists by special law).

### 16 Enforcement and Sanctions

#### 16.1 Describe the enforcement powers of the data protection authority(ies).

<table>
<thead>
<tr>
<th>Investigatory Power</th>
<th>Civil/Administrative Sanction</th>
<th>Criminal Sanction</th>
</tr>
</thead>
<tbody>
<tr>
<td>Non-compliance with notification of data processing/compliance in breach of the terms set out in article 23 of the LPDP, providing false information, after notification by the GPDP and maintaining access to open data transmission networks for the data controllers which do not comply with the provisions of the LPDP.</td>
<td>A fine of between 2,000 and 20,000 MOP for individuals and a fine of between 10,000 and 100,000 MOP for legal persons; the fines are increased to twice the amount indicated above if the data are subject to prior authorisation.</td>
<td>N/A</td>
</tr>
<tr>
<td>Non-compliance with stipulations of the LPDP regarding:</td>
<td>A fine of between 4,000 and 40,000 MOP.</td>
<td>N/A</td>
</tr>
<tr>
<td>1) data quality (article 5); 2) right to information, access, objection, right not to be subject to automated individual decisions (articles 10 to 13); 3) special security measures (article 16); 4) processing by subcontractor (article 17); and 5) non-provision of mandatory information provided in article 24, paragraph 1.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Non-compliance with stipulations of the LPDP regarding:</td>
<td>A fine of between 8,000 and 80,000 MOP.</td>
<td>N/A</td>
</tr>
<tr>
<td>1) conditions for legitimacy of data processing (article 6); 2) processing of sensitive data (article 7); 3) suspicions of illegal activities, criminal offences and administrative offences (article 8); 4) interconnection of personal data (article 9); and 5) transfer of data to a destination outside the MSAR and respective exemptions (articles 19 and 20).</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Non-compliance with stipulations of the LPDP regarding:</td>
<td>N/A</td>
<td>Imprisonment of up to one year or a fine of up to 120 days. The sanction is increased to twice the duration indicated above if the data involves sensitive data (article 7 of the LPDP) or suspicions of illegal activities, criminal offences and administrative offences (article 8 of the LPDP).</td>
</tr>
<tr>
<td>1) purposely omitting the notification/authorisation indicated in articles 21 and 22 of the LPDP; 2) providing false information in the notification/authorisation requests for the processing of personal data or making modifications in this request not allowed by the instrument of legalisation; 3) diverting or using personal data, in a manner incompatible with the purpose of the collection or with the instrument of legalisation; 4) promoting or carrying out an illegal interconnection of personal data; 5) non-compliance with the obligations provided for in this law or in other data protection legislation in the period established by the GPDP; and 6) maintaining access to open data transmission networks for those responsible for the processing of personal data that do not comply with the provisions of this law, after notification of the GPDP, not to do so.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Investigatory Power

<table>
<thead>
<tr>
<th>Civil/Administrative Sanction</th>
<th>Criminal Sanction</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access in any way to personal data whose access is forbidden to said individual/entity. The sanction is increased to twice the duration indicated when access: ■ is achieved through violation of technical safety rules; ■ has allowed the agent or third parties the obtainment of personal data; or ■ has provided the agent or third parties with a benefit or patrimonial advantage. Deletion, destruction, damaging, suppression or modification of personal data without proper authorisation, rendering the data unusable or affecting their ability to be used. Qualified disobedience regarding notification to interrupt, cease or block the processing of personal data, or in cases of: ■ refusal, without just cause, to cooperate as specifically requested by the GPDP; ■ refusal to totally or partially destroy personal data; and/or ■ refusal to destroy personal data, after the period of conservation provided for in the LPDP.</td>
<td>N/A</td>
</tr>
</tbody>
</table>

16.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?

The GPDP, as the public authority referred to in the LPDP (as well as in article 79 of the Macau Civil Code), carries out the tasks conferred upon it and is (inter alia) responsible for the supervision and coordination of compliance with and enforcement of the LPDP, as well as for the establishment of the secrecy regime and supervision of its execution.

The GPDP is also responsible for encouraging and supporting the development of codes of conduct designed to contribute, depending on the characteristics of the different sectors, to the proper implementation of the provisions of the LPDP and, in general, to greater effectiveness of self-regulation and protection of fundamental rights related to the protection of privacy.

As no specific provision exists regarding the possibility of the GPDP issuing a ban on a particular processing activity, and without prejudice to the guidelines that the GPDP may establish, we are of the view that such possibility is not within the powers of the public authority.

16.3 Describe the data protection authority’s approach to exercising those powers, with examples of recent cases.

Please note that, to the best of our knowledge, such data is not publicly available.

16.4 Does the data protection authority ever exercise its powers against businesses established in other jurisdictions? If so, how is this enforced?

Please note that, to the best of our knowledge, such data is not publicly available.

17 E-discovery / Disclosure to Foreign Law Enforcement Agencies

17.1 How do businesses typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?

Please note that, to the best of our knowledge, such data is not publicly available.

17.2 What guidance has/have the data protection authority(ies) issued?

Please note that, to the best of our knowledge, such data is not publicly available.

18 Trends and Developments

18.1 What enforcement trends have emerged during the previous 12 months? Describe any relevant case law.

Please note that, to the best of our knowledge, no enforcement trends have been made publicly available.

However, the recent topics publicised by the GPDP concern the following cases concluded in 2018 (stemming from complaints to the data protection regulator):

- Receipt of various telephone calls for inquiries (investigation no. 0011/2016/IP).
- Sending of an interpellation letter for payment by the property management company to the previous workplace of the owner (investigation no. 0062/2016/IP).
- Acquisition of personal data through the commercial registry (investigation no. 0185/2016/IP).
- Registration of visitors’ personal data when entering a building (investigation no. 0091/2017/IP).
- Reading of a marriage record in the processing of a wedding transcription (investigation no. 0094/2017/IP).
18.2 What “hot topics” are currently a focus for the data protection regulator?

In 2018, the GPDP issued an opinion on the processing of personal data arising from the use of video recording cameras in police uniforms (investigation no. 0003/P/2018/GPDP), recommending a redrafting of the purposes of such recording under the LPDP.
1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

The Personal Data Protection Act 2010 (the “PDPA”) is the principal legislation in Malaysia. The PDPA regulates the processing of personal data in commercial transactions and provides for matters connected therewith and incidental thereto.

1.2 Is there any other general legislation that impacts data protection?

Apart from the PDPA, there is no other general legislation governing data protection.

1.3 Is there any sector-specific legislation that impacts data protection?

There are several sector-specific pieces of legislation and regulations which impact data protection, including the following:

Banking and Financial Sector

The Personal Data Protection Code of Practice for Banking and Financial Sector was approved and registered by the Personal Data Protection Commissioner (the “Commissioner”) on 19 January 2017, which regulates the personal data processing activities carried out by members of the banking and financial sector.

Additionally, banking secrecy provisions are provided in the Financial Services Act 2013 (Islamic Financial Services Act 2013), which prohibit financial institutions and officers of a financial institution from disclosing customer information to any person. In addition, the Central Bank of Malaysia (Bank Negara Malaysia or “BNM”) has issued a number of guidelines and policy documents which address the obligations of financial institutions in respect of management of customer information; e.g., the standard of controls and security measures that a financial institution must have in place to protect customer information.

Communications Sector

The Personal Data Protection Code of Practice for the Communications Sector was approved and registered by the Commissioner on 23 November 2017, which regulates the personal data processing activities carried out by members of the communications sector.

Additionally, the Communications and Multimedia Consumer Forum of Malaysia (Consumer Forum) has issued the General Consumer Code of Practice for the Communications and Multimedia Industry Malaysia (the “Consumer Code”). The Consumer Code applies to all licensed service providers and members of the Consumer Forum and requires code subjects to maintain the privacy of identifiable information of a subscriber of telecommunications services. In particular, it addresses data protection principles such as notice and disclosure, consent, data security, data quality and access to personally identifiable information.

Healthcare Sector

The Private Healthcare Facilities and Services Act 1998 provides generally for the confidentiality of patients’ personal data and allows the Minister of Health to prescribe rules relating to “patients’ privacy, confidentiality and access to patients’ medical reports and records”. Additionally, the Private Health-care Facilities and Services (Private Hospitals and Other Private Healthcare Facilities) Regulations 2006 provide that all licensees under the said legislation must ensure that all original patients’ medical records and other related documents must be preserved for at least the relevant limitation period (that is, for a minimum of six years).

1.4 What authority(ies) are responsible for data protection?

The Personal Data Protection Commissioner is responsible for implementing and enforcing the PDPA.

The Commissioner is assisted by the Personal Data Protection Department (Jabatan Perlindungan Data Peribadi or “JPDP”), which is a department established by the Ministry of Communications and Multimedia in Malaysia.

2 Definitions

2.1 Please provide the key definitions used in the relevant legislation:

- “Personal Data” means any information in respect of commercial transactions, which:
  (a) is being processed wholly or partly by means of equipment operating automatically in response to instructions given for that purpose;
  (b) is recorded with the intention that it should wholly or partly be processed by means of such equipment; or
is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system, that relates directly or indirectly to a data subject, who is identified or identifiable from that information or from that and other information in the possession of a data user, including any sensitive personal data and expression of opinion about the data subject, but does not include any information that is processed for the purpose of a credit reporting business carried on by a credit reporting agency under the Credit Reporting Agencies Act 2010.

- “Processing”, in relation to personal data, means collecting, recording, holding or storing the personal data or carrying out any operation or set of operations on the personal data, including:
  - (a) the organisation, adaptation or alteration of personal data;
  - (b) the retrieval, consultation or use of personal data;
  - (c) the disclosure of personal data by transmission, transfer, dissemination or otherwise making available; or
  - (d) the alignment, combination, correction, erasure or destruction of personal data.

- “Controller”. The term used in Malaysia is “data user”. A “data user” is defined as a person who either alone or jointly or in common with other persons processes any personal data or has control over or authorises the processing of any personal data, but does not include a data processor.

- “Processor” means any person, other than an employee of the data user, who processes the personal data solely on behalf of the data user, and does not process the personal data for any of his own purposes.

- “Data Subject” means an individual who is the subject of the personal data.

- “Sensitive Personal Data” means any personal data consisting of information as to the physical or mental health or condition of a data subject, his political opinions, his religious beliefs or other beliefs of a similar nature, the commission or alleged commission by him of any offence or any other personal data as may be determined by the Minister of Communications and Multimedia.

- “Data Breach” is not defined in the PDPA.

- Other key definitions – please specify (e.g., “Pseudonymous Data”, “Direct Personal Data”, “Indirect Personal Data”).

The PDPA applies only in respect of personal data processed in “commercial transactions”.

“Commercial transactions” are defined as any transaction of a commercial nature, whether contractual or not, which includes any matters relating to the supply or exchange of goods or services, agency, investments, financing, banking and insurance, but does not include a credit reporting business carried out by a credit reporting agency under the Credit Reporting Agencies Act 2010.

### 3 Territorial Scope

**3.1 Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to those laws?**

Generally, the PDPA does not apply to any personal data processed outside Malaysia, unless the personal data is intended to be further processed in Malaysia. In addition, the PDPA will apply to a business established outside Malaysia where the business uses equipment in Malaysia for the processing of personal data other than for the purposes of transit of the personal data through Malaysia. In this instance, the business shall be required to nominate a representative established in Malaysia.

### 4 Key Principles

**4.1 What are the key principles that apply to the processing of personal data?**

- **Transparency**
  This is provided under section 7 of the PDPA (Notice and Choice Principle). This Principle provides that the data user shall provide its data subjects with a written notice which essentially informs them how their personal data will be processed by the data user. Section 7 of the PDPA identifies the specific types of information which must be included in such written notice.

- **Lawful basis for processing**
  This is provided under section 6 of the PDPA (General Principle). This Principle provides that personal data shall not be processed unless with the consent of the data subject. However, a data user may process personal data without the consent of the data subject where the consent requirement is exempted under the PDPA; for example, where processing is necessary for performance of a contract involving the data subject, to take steps with a view of entering into a contract at the data subject’s request, to comply with any legal obligation, to protect the vital interests of the data subject, etc.

- **Purpose limitation**
  The General Principle further provides that personal data shall not be processed unless the processing in question is:
  - for a lawful purpose directly related to an activity of the data user;
  - necessary for or directly related to that purpose; and
  - adequate but not excessive in relation to that purpose.

- **Data minimisation**
  Please refer to our response to the section on “Purpose limitation” above.

- **Proportionality**
  Please refer to our response to the section on “Purpose limitation” above.

- **Retention**
  Section 10 of the PDPA (Retention Principle) provides that personal data processed for any purpose shall not be kept longer than is necessary for the fulfilment of the purpose. Businesses should note that the application of this principle must be considered against any applicable statutory retention period which may apply to the personal data, where the personal data may need to be retained for compliance with applicable laws.

Where personal data is no longer needed for the purpose it was collected, the business must ensure the personal data is destroyed or permanently deleted.

- **Other key principles – please specify**
  - **Security**
    Section 9 of the PDPA (Security Principle) provides that data users must take practical steps to protect personal data from any loss, misuse, modification, unauthorised or accidental access or disclosure, alteration or destruction, by deployment of the necessary technical or organisational security measures to protect personal data.

Where processing is carried out by a data processor, the data user is required to ensure the data processor shall (i) provide
sufficient guarantees in respect of the technical and organisational security measures governing the processing to be carried out, and (ii) take reasonable steps to ensure compliance with those measures.

- **Data Integrity**
  Section 11 of the PDPA (Data Integrity Principle) requires data users to take reasonable steps to ensure that personal data in their possession is accurate, complete, not misleading and kept up to date, having regard to the purpose for which the personal data was collected.

- **Disclosure**
  Section 8 of the PDPA (Disclosure Principle) states that, without the consent of the data subject, no personal data shall be disclosed:
  - for any purpose other than the purpose for which the personal data was to be disclosed at the time the personal data was collected; or
  - to any party which does not belong to one of the classes of third parties identified in the Privacy Notice, as one of the classes of third parties to whom the data user may disclose personal data.

- **Access**
  Section 12 of the PDPA (Access Principle) requires data subjects to be provided the right to access his personal data and be able to correct his personal data where the personal data is inaccurate, incomplete, misleading or not up-to-date.

### 5 Individual Rights

#### 5.1 What are the key rights that individuals have in relation to the processing of their personal data?

- **Right to access to data/copies of data**
  Data subjects have the right to be informed as to whether his/her personal data is being processed by or on behalf of the data user and may request to be provided with a copy of his/her personal data.
  
  In certain circumstances identified in the PDPA, the data user has the right to refuse to comply with the data access request.

- **Right to rectification of errors**
  Where a data subject considers or knows that his personal data held by the data user is inaccurate, incomplete, misleading or not up to date, the data subject is entitled to request the data user to make the necessary correction to the personal data.
  
  In certain circumstances identified in the PDPA, the data user has the right to refuse to comply with the data correction request.

- **Right to deletion/right to be forgotten**
  No similar right under the PDPA.

- **Right to object to processing**
  A data subject may require the data user to cease the processing or not begin the processing of any personal data relating to him if the said processing is causing or is likely to cause substantial damage or substantial distress to him or to another person and the damage or distress is or would be unwarranted.

- **Right to restrict processing**
  There is no similar right under the PDPA.

- **Right to data portability**
  There is no similar right under the PDPA.

- **Right to withdraw consent**
  A data subject may, by notice in writing, withdraw his consent to the processing of personal data in respect of which he is the data subject.

- **Right to object to marketing**
  A data subject may, at any time, require the data user to cease or not to begin processing his/her personal data for purposes of “direct marketing”, i.e. the “communication by whatever means of any advertising or marketing material which is directed to particular individuals”.

- **Right to complain to the relevant data protection authority(ies)**
  Any individual or relevant person may make a complaint in writing to the Commissioner about an act, practice or request specified in the complaint that relates to personal data of which the individual is the data subject and may be in contravention of the PDPA.

### 6 Registration Formalities and Prior Approval

#### 6.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?

The Personal Data Protection (Class of Data Users) Order 2013 (as amended by the Personal Data Protection (Class of Data Users) (Amendment) Order 2016) identifies 13 classes of data users which are required to register with the Commissioner, including licensed or regulated businesses in the following sectors:

- Communications.
- Banking and financial institutions.
- Insurance.
- Health.
- Tourism and hospitality.
- Transportation (that is, specifically identified airlines).
- Education.
- Direct selling.
- Services (that is, certain service providers only).
- Real estate.
- Utilities.
- Pawnbrokers.
- Moneylenders.

#### 6.2 If such registration/notification is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?

While there is no explicit requirement for the information provided to be specific and exhaustive, the Commissioner generally requires the data users who are required to be registered under the PDPA to provide a list of the categories of personal data, the purposes for processing personal data, third parties to whom personal data may be disclosed to, etc.

Please refer to the list in question 6.5 for the types of information which must be submitted as part of the registration process.
6.3 On what basis are registrations/notifications made (e.g., per legal entity, per processing purpose, per data category, per system or database)?

Each legal entity which falls within any of the classes of data users requiring registration under the PDPA must apply for registration with the Commissioner. A data user who belongs to two or more classes must make an application separately for each class to which that data user belongs.

6.4 Who must register with/notify the data protection authority (e.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation)?

Pursuant to the Personal Data Protection (Class of Data Users) Order 2013, a data user (i.e. a legal entity) which falls within any of the prescribed classes of data users must register with the Commissioner. Generally, the entity which holds the relevant licence or approval, based on the respective sectors as identified in the Order, must register with the Commissioner.

6.5 What information must be included in the registration/notification (e.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes)?

Registration with the Commissioner is done online, by filling in an online registration form which can be found at the JPDP’s official website.

The online registration form consists of six parts:
- Name and business details – general information and the contact details of the data user, the type of business conducted and the class/sector of the data user.
- Purpose – the nature/purpose of the data user and any additional purposes for the processing of personal data.
- Description – a listing of the types of personal data that are processed in connection with the purposes cited in the form.
- Disclosure – to identify the parties to whom personal data is disclosed.
- Transfer Abroad – to identify countries to which transfers of personal data take place, along with a description of the data to be transferred and the purpose of the transfer.
- Compliance Person – details of the officer who will supervise the registration of personal data on behalf of the data user organisation.

6.6 What are the sanctions for failure to register/notify where required?

Data users falling within one of the classes of data users as set out in question 6.1 above, and who fail to register with the Commissioner, shall commit an offence which renders the data user liable, upon conviction, to a fine not exceeding RM500,000 and/or imprisonment for up to three years.

6.7 What is the fee per registration/notification (if applicable)?

The fee for registration is based on the types of business, as follows:
- Sole proprietorship: RM100.
- Partnership: RM200.
- Private limited company: RM300.
- Public limited company: RM400.

6.8 How frequently must registrations/notifications be renewed (if applicable)?

The certificate of registration is valid for a period of not less than 12 months from the date on which the certificate was issued. Data users are obliged to renew the certificate no later than 90 days before the expiry of the certificate. Failure to renew the certificate and continued processing of personal data after the expiry of the certificate is an offence which renders the data user liable, upon conviction, to a fine not exceeding RM250,000 and/or imprisonment for up to two years.

6.9 Is any prior approval required from the data protection regulator?

Yes, prior approval is required.

6.10 Can the registration/notification be completed online?

Yes, the registration can be completed online.

6.11 Is there a publicly available list of completed registrations/notifications?

While the Commissioner is required under the PDPA to maintain a Register of Data Users, this listing is not made publicly available. However, any person may, upon request and payment of a fee, access the register and make copies or take relevant extracts from an entry in the register.

6.12 How long does a typical registration/notification process take?

Typically, it takes less than two months for a registration process to be completed.

7 Appointment of a Data Protection Officer

7.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.

The appointment of a Data Protection Officer is currently optional under the PDPA. Notwithstanding the above, the PDPA requires the data user to provide data subjects with its contact details, in order to respond to any inquiries or complaints regarding the processing of his personal data, and such details must include at least the following:
- designation of the contact person for the data user;
- phone number;
- fax number (if any);
- e-mail address (if any); and
- other related information.
7.2 What are the sanctions for failing to appoint a Data Protection Officer where required?

This is not applicable in Malaysia.

7.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect of his or her role as a Data Protection Officer?

This is not applicable in Malaysia.

7.4 Can a business appoint a single Data Protection Officer to cover multiple entities?

This is not applicable in Malaysia.

7.5 Please describe any specific qualifications for the Data Protection Officer required by law.

This is not applicable in Malaysia.

7.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?

This is not applicable in Malaysia.

7.7 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?

This is not applicable in Malaysia.

7.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?

As stated in our response to question 7.1 above, the PDPA requires the data user to provide data subjects with its contact details in order to respond to any inquiries or complaints. This is to be provided in the data user’s privacy notice or such other relevant written notice to the data subject.

8 Appointment of Processors

8.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?

Yes. Where processing of personal data is carried out by a data processor for or on behalf of the business, the business must enter into a contract to bind such data processor in respect of its operating activities and its carrying out of personal data processing activities, in order to ensure the security of personal data.

In connection with this, the business must ensure that the data processor provides sufficient guarantees in respect of the technical and organisational security measures governing the processing to be carried out, and to take reasonable steps to ensure the data processor’s compliance with those measures.

8.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?

There are no prescribed formalities with regards to the agreement to be entered into with the data processor. However, in view of the fact that the data user will be primarily responsible for any non-compliance or breach by the data processor with regards to the personal data, it would be prudent for the data user to impose equivalent if not more stringent data protection obligations upon its data processors. At the minimum, the agreement should address the following:

(a) the data processor must provide sufficient guarantees in respect of the technical and organisational security measures to be carried out;

(b) the data user should be given audit rights, in order to ensure the data processor’s compliance with the abovementioned measures; and

(c) specific or minimum technical and organisational security measures governing the processing should be provided in the agreement. On this note, the data processor must be made to comply with the minimum security standards provided under the Personal Data Protection Standards 2015, or such other standards or guidelines to be issued by the Commissioner from time to time.

9 Marketing

9.1 Please describe any legislative restrictions on the sending of electronic direct marketing (e.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient)?

Pursuant to section 43 of the PDPA, a data subject may, at any time by notice in writing to a data user, require the data user to cease or not to begin processing his personal data for purposes of direct marketing. The data user must comply with such notice by the end of such period as is reasonable in the circumstances.

In this regard, the Commissioner has also released a Public Consultation Paper (No. 1/2014) titled the Guide In Dealing With Direct Marketing Under Personal Data Protection Act (PDPA) 2010 (the “Direct Marketing Public Consultation Paper”). The Direct Marketing Public Consultation Paper provides that a data user is not allowed to use electronic communications for direct marketing except in situations where:

(a) the data subjects have given explicit consent to do so;

(b) personal data of individuals have been obtained in the course of sale of products or services;

(c) the data subjects have been informed of the identity of the direct marketing organisations, purpose of collecting the personal data and the persons to whom the said personal data may be disclosed;

(d) materials of the direct marketing to be given are limited to similar products and services only; and

(e) means of refusing the use of the data subjects’ personal data for direct marketing purposes are provided. For example, an opt-out right must be made available on every subsequent marketing message.

To date, the Commissioner has not officially issued the Direct Marketing Public Consultation Paper, and therefore it has not yet come into legal effect.
9.2 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.).

With regard to postal direct marketing, mail received through home or office letter boxes will be considered as direct marketing if it meets two criteria: (i) it must be addressed to a named person; and (ii) it must be about product or service promotion. There are no restrictions with regards to unaddressed mails such as those addressed to “the occupant”, “the resident” or “the houseowner” which do not involve the use of personal data.

9.3 Do the restrictions noted above apply to marketing sent from other jurisdictions?

The restrictions above will not apply to marketing sent from other jurisdictions to data subjects in Malaysia, unless the relevant data user is based in Malaysia.

9.4 Is/are the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?

There are no reported cases of the Commissioner actively enforcing against breaches of marketing restrictions in Malaysia. However, the Direct Marketing Public Consultation Paper (which has yet to come into legal force) provides guidance to data subjects in respect of lodging complaints with the Commissioner on direct marketing activities which are not in compliance with the PDPA.

Further to this, in September 2018, the Commissioner issued template forms which may be used by a data subject (i) to prevent data users from processing the personal data of the data subject for the purpose of direct marketing, and (ii) to lodge a complaint with the Commissioner where the data user does not cease the said processing.

9.5 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?

There are no prohibitions under the PDPA against purchasing marketing lists from third parties. However, to avoid any complication in respect of the source of the marketing lists obtained from third parties (and in respect of the individuals whose personal data are contained in such marketing lists), it would be advisable for the business to obtain adequate warranties and indemnities from the third parties selling the marketing lists, to ensure that the individuals have provided their consent to receiving marketing materials from the business, or at the very least the individuals must not have clearly indicated that they do not consent to the receipt of any marketing materials.

9.6 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?

Failure to comply with the direct marketing provisions under the PDPA may render the business liable, upon conviction, to a fine not exceeding RM200,000 and/or to imprisonment for a term not exceeding two years.

10 Cookies

10.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).

There are no legislative restrictions on the use of cookies (or similar technologies) under the PDPA. However, insofar as the cookies (or similar technologies) contain personal data, these will fall within the ambit of “personal data” and therefore be subjected to the personal data protection key principles and other requirements under the PDPA.

10.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?

This is not applicable in Malaysia.

10.3 To date, has/have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?

None that we are aware of.

10.4 What are the maximum penalties for breaches of applicable cookie restrictions?

This is not applicable in Malaysia, as there are no cookie-specific restrictions under the PDPA.

11 Restrictions on International Data Transfers

11.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.

The PDPA prohibits the transfer of any personal data of a data subject to a place outside Malaysia unless to such place as specified by the Communications and Multimedia Minister, upon the recommendation of the Commissioner, and by notification published in the Gazette. In May 2017, the Commissioner published on its official website the Public Consultation Paper No. 1/2017 titled the Personal Data Protection (Transfer of Personal Data to Places outside Malaysia) Order 2017 (the “Proposed Order”). The Proposed Order is essentially a “White List” which permits the transfer of personal data to certain jurisdictions outside Malaysia. The “White List” places identified by the Commissioner are as follows:

(a) European Economic Area (EEA) member countries.
(b) United Kingdom.
(c) The United States of America.
(d) Canada.
(e) Switzerland.
(f) New Zealand.
(g) Argentina.
(h) Uruguay.
(i) Andorra.
(j) Faroe Islands.
(k) Guernsey.
(l) Israel.
(m) Isle of Man.
(n) Jersey.
(o) Australia.
(p) Japan.
(q) Korea.
(r) China.
(s) Hong Kong.
(t) Taiwan.
(u) Singapore.
(v) The Philippines.
(w) Dubai International Financial Centre (DIFC).
Notwithstanding the foregoing, as of the date of this edition, the Commissioner has yet to officially issue the Proposed Order, and therefore the Proposed Order has not yet come into legal effect.

11.2 Please describe the mechanisms businesses typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).

As the Proposed Order has not yet come into legal effect, section 129(3) of the PDPA provides circumstances under which a business is permitted to transfer personal data outside of Malaysia, including where:

(a) the data subject has consented to the transfer;
(b) the transfer is necessary for the performance of contract between the data subject and the business;
(c) the transfer is necessary for the conclusion or performance of a contract between the business and a third party which is entered into at the request of the data subject or in the interests of the data subject;
(d) the transfer is for the purpose of any legal proceedings or for the purpose of obtaining legal advice or for establishing, exercising or defending legal rights;
(e) the business has reasonable grounds for believing that in all circumstances of the case, the transfer is for the avoidance or mitigation of adverse action against the data subject, it is not practicable to obtain the consent in writing of the data subject to that transfer and if it was practicable to obtain such consent, the data subject would have given the consent;
(f) the business has taken all reasonable precautions and exercised all due diligence to ensure that the personal data will not in that place be processed in any manner which contravenes the PDPA;
(g) the transfer is in order to protect the vital interests of the data subject; or
(h) the transfer is in the public interest under circumstances determined by the Minister.

11.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.

No; neither registration/notification nor prior approval is required.

12 Whistle-blower Hotlines

12.1 What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?

There are no specific laws or regulations setting out the permitted scope of corporate whistle-blower hotlines. However, the primary legislation regulating the conduct of whistle-blowing in Malaysia is the Whistleblower Protection Act 2010 (the “WPA”). Generally, the WPA provides protection to the whistle-blower including (i) protection of the identity of the whistle-blower, (ii) immunity from civil and criminal action, and (iii) protection against detrimental action.

However, the protection conferred by the WPA only applies where the whistle-blowing in question fulfils each of the following conditions:

(a) the disclosure of improper conduct was made to one of the seven enforcement agencies identified;
(b) the disclosure made is not specifically prohibited by any written law; and
(c) none of the situations identified in section 11 of the WPA (which makes it mandatory for whistle-blower protection to be revoked in the situations identified) apply.

In respect of (b) above, some examples of disclosures which are specifically prohibited by written laws include disclosures of official secrets as defined under the Official Secrets Act 1972. In addition, section 203A of the Penal Code makes it an offence for civil servants to disclose information “in the performance of his duties or the exercise of his functions under any written law”.

12.2 Is anonymous reporting prohibited, strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do businesses typically address this issue?

Whistle-blowing laws are silent on anonymous reporting. However, given that whistle-blowing in general is encouraged (and is even mandatory in some instances), it is unlikely that anonymous reporting would be prohibited. For example, the WPA expressly states that the purpose of the WPA is “to combat corruption and other wrongdoings by encouraging and facilitating disclosures of improper conduct in the public and private sector, to protect persons making those disclosures from detrimental action, to provide for the matters disclosed to be investigated and dealt with and to provide for other matters connected therewith” (emphasis added).

Specific to businesses, the Companies Act 2016 (the “CA”) creates a mandatory duty for auditors of a company to report breaches of the CA, as well as suspected commissions of serious offences by officers of a company against the company, to the Companies Commission of Malaysia (“CCM”). The CA protects auditors of a company, as well as other officers of a company against any action or proceeding arising from the making of such disclosures to the CCM.

Similarly, the Capital Markets and Services Act 2007 (the “CMSA”) creates a mandatory duty for auditors of listed corporations to report any breach of securities laws, or of the Bursa Malaysia listing rules, to the Securities Commission and Bursa Malaysia. Any auditor, chief executive officer or other officer responsible for preparing or approving financial statements or financial information, or a secretary of a listed corporation making said report is protected under the CMSA. The CMSA provides that a listed corporation shall not remove, discriminate, demote, suspend or interfere with the lawful employment or livelihood of such persons because of their reporting.
### 13 CCTV

#### 13.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice?

No. However, based on the Public Consultation Paper (No.5/2014) titled the Guide on The Management of CCTV Under Personal Data Protection Act (PDPA) 2010 (“CCTV Guide”), which has yet to come into legal force, businesses or owners of premises with installed CCTV have the responsibility to display a notice that is visible to visitors and to place such notice at the entrance to the CCTV surveillance zone, in order to inform them of the CCTV operation and the purposes for such installation.

#### 13.2 Are there limits on the purposes for which CCTV data may be used?

There are no specific limits imposed upon the purposes for which CCTV data may be used. However, the CCTV Guide provides guidance as to the purposes for installation and use of CCTV, whereby businesses may install CCTV for the purpose of prevention or detection of crime or for the purpose of investigation (as these purposes are permitted pursuant to section 45 of the PDPA). However, for purposes other than the foregoing, consent is required from an individual for any of his recorded images to be used in commercial transactions.

### 14 Employee Monitoring

#### 14.1 What types of employee monitoring are permitted (if any), and in what circumstances?

The PDPA does not specifically prohibit employee monitoring. However, the CCTV Guide (as described in question 13.1 above), which was published by the Commissioner in 2014 but has yet to come into legal force as at the time of writing, provides that installation of CCTV cannot be misused for the purpose of staff monitoring.

#### 14.2 Is consent or notice required? Describe how employers typically obtain consent or provide notice.

The business would need to provide notice and obtain consent from the employees. Employers generally obtain consent by incorporating the relevant terms in the employment contracts, employment handbook, policies or manuals, which must be accepted by the employees prior to or at the time of employment.

#### 14.3 To what extent do works councils/ trade unions/employee representatives need to be notified or consulted?

This is not applicable in Malaysia.

### 15 Data Security and Data Breach

#### 15.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?

Yes. The data user has a general obligation to ensure the security of the personal data in accordance with section 9 of the PDPA (Security Principle). The data user must also comply with the minimum security standards as prescribed under the Personal Data Protection Standards 2015.

Furthermore, where processing of personal data is carried out by a data processor for or on behalf of the data user, the data user is responsible to ensure that the data processor provides sufficient guarantees in respect of the technical and organisational security measures governing the processing to be carried out, and to take reasonable steps to ensure compliance with those measures.

#### 15.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

There is currently no legal requirement to report data breaches to the Commissioner.

However, in August 2018, the Commissioner issued a Public Consultation Paper (No. 1/2018) titled The Implementation of Data Breach Notification (“DBN Public Consultation Paper”) with the aim of soliciting feedback from the public in relation to the proposed implementation of a data breach notification (“DBN”) mechanism in Malaysia. Once the DBN Public Consultation Paper is officially issued and comes into legal effect, data users will be required to notify and inform the relevant authorities (including the Commissioner) and the affected parties when a data breach has occurred within the organisation.

The contents of the DBN shall include:

(i) details about the incident, (i.e. a summary of the event and circumstances, type and amount of personal data involved in the incident and the estimated number of affected individuals);

(ii) the organisation’s containment or control measures (i.e. details of actions/measures taken or to be taken to contain the breach and the potential harm of the breach, especially to the affected individuals);

(iii) details and requirements with regards to notification (i.e. identification of the persons who have been notified about the breach, details of whether any regulatory bodies/law enforcement agencies have been notified about the breach, the method(s) used by the organisation to notify affected individuals about the incident, any advice given to the affected individual(s), and the requirement for the Commissioner to be notified no later than 72 hours after having become aware of the breach); and

(iv) details on the organisations’ training and guidance in relation to data protection (i.e. whether the organisation had provided training/awareness programmes to staff members prior to the incident, whether the staff members involved in the incident had received training in the last 24 months and whether the organisation had provided any detailed guidance to staff on the handling of personal data in relation to the reported incident).
Notwithstanding the foregoing, as of the date of this edition, the Commissioner has not officially issued the DBN Public Consultation Paper, and it has therefore not yet come into legal effect.

15.3 Is there a legal requirement to report data breaches to affected data subjects? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

Please see answer to question 15.2 above. The DBN Public Consultation Papers requires data users to provide the information below to the affected data subjects, including:

(i) details of actions/measures taken or to be taken to contain the breach;
(ii) advice given to the affected individual; and
(iii) the potential harm of the breach on the affected individuals.

15.4 What are the maximum penalties for data security breaches?

This is not applicable in Malaysia, as the DBN Public Consultation Paper has not yet come into legal effect and the Commissioner has not clarified the repercussions of non-compliance (should the Public Consultation Paper come into legal effect).

16 Enforcement and Sanctions

16.1 Describe the enforcement powers of the data protection authority(ies).

<table>
<thead>
<tr>
<th>Investigatory Power</th>
<th>Civil/Administrative Sanction</th>
<th>Criminal Sanction</th>
</tr>
</thead>
<tbody>
<tr>
<td>Investigation by the Commissioner</td>
<td>Where the Commissioner receives a complaint, the Commissioner shall carry out an investigation in relation to the relevant data user to ascertain whether the act, practice or request specified in the complaint contravenes the provisions of the PDPA.</td>
<td>Not applicable.</td>
</tr>
<tr>
<td>Search and seizure with or without warrant</td>
<td>The Magistrate may issue a warrant authorising the authorising officer at any reasonable time by day or night and with or without assistance, to enter the premises and if need be by force, if it appears to a Magistrate, upon written information on oath from the authorising officer and after such inquiry as the Magistrate considers necessary, that there is reasonable cause to believe that any premises has been used for or there is any premises evidence necessary to the conduct of an investigation of the commission of an offence under the PDPA. Notwithstanding that, search and seizure may be conducted without a warrant, if an authorising officer is satisfied upon information received that he has reasonable cause to believe that delaying the search warrant would be adversely affected or evidence of the commission of an offence is likely to be tampered with, removed, damaged or destroyed.</td>
<td>A person who breaks, tampers with or damages such evidence shall, on conviction, be liable to a fine not exceeding RM50,000 or imprisonment for a term not exceeding six months, or both.</td>
</tr>
<tr>
<td>Power to require production of computer, book, account, etc.</td>
<td>An authorised officer shall have the power to require the production of any computer, book, account, computerised data or other document kept by the data user or any other person and to inspect, examine and to download from them, make copies of them or take extracts from them, require the production of any identification document from any person in relation to any act or offence under the PDPA, and make such enquiries as may be necessary to ascertain whether the provisions of PDPA have been complied with.</td>
<td>Any person who refuses any access to any premise to which the authorised officer is entitled to, assaults, obstructs, hinders, or delays any authorised officer, or refuses any authorised officer any information relating to the offence, commits an offence and shall, on conviction, be liable to imprisonment for a term not exceeding two years or a fine not exceeding RM10,000 or both.</td>
</tr>
<tr>
<td>Power to require attendance of persons acquainted with the case</td>
<td>An authorised officer making an investigation under the PDPA may order in writing require the attendance before himself of any person who appears to the authorised officer to be acquainted with the facts and circumstances of the case, and such person shall attend as so required.</td>
<td>Similar to the above. Further, if any person refuses or fails to attend as required, the authorised officer may report such refusal or failure to a Magistrate, who shall issue a summons to secure the attendance of the person.</td>
</tr>
<tr>
<td>Examination of persons acquainted with the case</td>
<td>An authorised officer making an investigation under the PDPA may examine orally any person supposed to be acquainted with the facts and circumstances of the case and shall reduce into writing any statement made by the person so examined.</td>
<td>Similar to the above.</td>
</tr>
<tr>
<td>Power of arrest</td>
<td>An authorised officer or police officer may arrest without warrant any person whom he reasonably believes has committed or is attempting to commit an offence under the PDPA.</td>
<td>Similar to the above.</td>
</tr>
</tbody>
</table>
16.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?

While there is no specific power provided under the PDPA for the Commissioner to issue a ban on a particular activity, the Commissioner may, pursuant to section 108(1) of PDPA, serve on the relevant data user an enforcement notice to direct, where necessary, the relevant data user to cease processing the personal data pending the remedy of the contravention by the data user. A court order is not required for the issuance of such enforcement notice by the Commissioner.

16.3 Describe the data protection authority’s approach to exercising those powers, with examples of recent cases.

The Commissioner has been carrying out inspections on businesses from time to time with a view of providing recommendations to the businesses on their personal data protection practices and compliance with the PDPA.

On 3 May 2017, a local private college was the first data user to be charged in the Sessions Court for processing personal data of former employees of the college without a valid certificate of registration issued by the Commissioner, in contravention of section 16 of the PDPA. Other recent cases of enforcement by the Commissioner include actions against a hotel, a college and a recruitment agency for failure to register under the PDPA. These cases have resulted in imposition of fines ranging from RM10,000 to RM20,000 or in lieu of payment of the stipulated fines, imprisonment term of up to eight months.

16.4 Does the data protection authority ever exercise its powers against businesses established in other jurisdictions? If so, how is this enforced?

There has not been any reported case whereby the Commissioner exercises its powers against businesses established in other jurisdictions.

17 E-discovery / Disclosure to Foreign Law Enforcement Agencies

17.1 How do businesses typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?

There is no standard or typical response by businesses to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies.

However, businesses may consider providing in their privacy notices or policies that where required by any law or any enforcement authority, both inside or outside Malaysia, the businesses may disclose an individual’s personal data to the extent necessary to comply with any law or enforcement authority.

17.2 What guidance has/have the data protection authority(ies) issued?

As of the date of this edition, the Commissioner has not issued any specific guidance on this issue.

18 Trends and Developments

18.1 What enforcement trends have emerged during the previous 12 months? Describe any relevant case law.

Based on the Commissioner’s enforcement activities and reported cases published in its official website, the Commissioner has been actively carrying out inspections on various businesses, particularly businesses which fall within the classes of data users requiring registration under the PDPA (see question 6.1 above).

Reported cases of offences under the PDPA are also listed in the Commissioner’s official website, where it can be observed that most of the cases in the previous 12 months involve non-compliance of data users with the registration requirement of the PDPA, where such data users fall within the classes of data users requiring registration under the PDPA.

18.2 What “hot topics” are currently a focus for the data protection regulator?

As stated in question 15.2 above, the Commissioner recently issued the DBN Public Consultation Paper, and therefore is aiming to implement a data breach notification regime mechanism in Malaysia in the near future.

Apart from the above, the incumbent Communications and Multimedia Minister has issued a statement that the Ministry is currently looking into carrying out a comprehensive review and amendment of the PDPA in the year 2019, with the aim of aligning the PDPA with the European Union General Data Protection Regulation (“GDPR”).
Deepak Pillai
Christopher & Lee Ong
Level 22 Axiata Tower
No. 9 Jalan Stesen Sentral 5
Kuala Lumpur Sentral
50470 Kuala Lumpur
Malaysia
Tel: +60 3 2267 2675
Email: deepak.pillai@christopherleeong.com
URL: www.christopherleeong.com

Deepak has practised exclusively in TMT & Data Protection for two decades and is acknowledged as a leading TMT & Data Protection lawyer in Malaysia.
Deepak advises clients on matters relating to IT contracts, electronic commerce, online financial services, outsourcing, telecommunications, IT security, personal data protection and digital media. He advises a wide array of international, private and public sector clientele in addressing the commercial, regulatory and policy issues relating to information and communications technology law.
Deepak has been described in The Legal 500 over the years as "pioneering the practice of IT law as a discrete area of law in Malaysia" and "the most recognised IT specialist in Malaysia". Deepak has been listed by The Legal 500 Asia Pacific as a leading individual in the area of IT and Telecommunications from 2001 to date, and is the sole Malaysian lawyer ranked in Band 1 for TMT in Chambers Asia-Pacific 2019.

Yong Shih Han
Christopher & Lee Ong
Level 22 Axiata Tower
No. 9 Jalan Stesen Sentral 5
Kuala Lumpur Sentral
50470 Kuala Lumpur
Malaysia
Tel: +60 3 2267 2715
Email: shih.han.yong@christopherleeong.com
URL: www.christopherleeong.com

Shih Han practices exclusively in the areas of Technology, Media and Telecommunications ("TMT"), and Data Protection. Prior to joining the firm, she was a dispute resolution associate in a reputable firm, handling primarily civil and corporate litigation matters. Since joining the firm and making the transition to corporate practice, she has been involved in the areas of corporate commercial, mergers & acquisitions, and general corporate advisory. She currently focuses on the areas of technology, media, telecommunications and data protection, with information security and data protection being her specialised area.
She now regularly advises clients on matters relating to information and communications technology, information security and data protection, telecommunications, and media and advertising laws. This ranges from the preparation and drafting of technology-related contracts and policies to advising clients on matters potentially leading to dispute resolution. She also regularly advises clients on technology- and media-related regulatory and compliance matters.
Shih Han has been listed by The Legal 500 Asia Pacific as a next-generation lawyer in the area of IT and Telecommunications in 2019.

CHRISTOPHER & LEE ONG

Christopher & Lee Ong ("CLO") is one of Malaysia’s most established and respected law firms, providing high-quality advice to clients across the commercial spectrum, with extensive experience in handling complex deals and disputes involving large local and multinational corporations, and governments and their agencies, as well as smaller local enterprises.
CLO’s technology, media & telecommunications ("TMT") practice group is one of the most established and respected practices in the Asia Pacific region. With clients ranging from state governments and statutory boards to multinational corporations in the telecommunications, computer hardware and software sectors, the firm has been involved in many of the largest and most complex IT and telecommunications projects in recent years. The firm regularly advises clients on matters relating to IT contracts, electronic and mobile commerce, online financial services, outsourcing, telecommunications, cybersecurity, personal data protection, as well as regulatory and policy issues relating to information and communications technology law.
The firm’s TMT practice group was named Technology, Media and Telecommunications Law Firm of the Year 2017 by Asian Legal Business at the Malaysian Law Awards.
1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?
As of 25 May 2018, the principal data protection legislation in the EU is Regulation (EU) 2016/679 (the “General Data Protection Regulation” or “GDPR”). The GDPR repealed Directive 95/46/EC (the “Data Protection Directive”) and led to increased (though not total) harmonisation of data protection law across the EU Member States.

The provisions of the GDPR are complemented by Maltese legislation, namely the Data Protection Act (“DPA”), Chapter 586 of the Laws of Malta and various pieces of subsidiary legislation implemented under the same Chapter 586.

1.2 Is there any other general legislation that impacts data protection?
General legislation which currently impacts data protection includes:
- Processing of Personal Data (Protection of Minors) Regulations (Subsidiary Legislation 586.04).
- Transfer of Personal Data to Third Countries Order (S.L. 586.05).
- Restriction of Data Protection (Obligations and Rights) Regulations (S.L. 586.09).

1.3 Is there any sector-specific legislation that impacts data protection?
Current sector-specific legislation relating to data protection includes:
- Processing of Personal Data (Electronic Communications Sector) Regulations (Subsidiary Legislation 586.01).
- Processing of Personal Data for the purposes of the General Elections Act and the Local Councils Act Regulations (Subsidiary Legislation 586.06).
- Processing of Personal Data (Education Sector) Regulations (Subsidiary Legislation 586.07).
- Data Protection (Processing of Personal Data by Competent Authorities for the Purposes of the Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties) Regulations (Subsidiary Legislation 586.08).

1.4 What authority(ies) are responsible for data protection?
The relevant data protection regulatory authority is the Information and Data Protection Commissioner (“IDPC”).

2 Definitions

2.1 Please provide the key definitions used in the relevant legislation:
- “Personal Data” means any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
- “Processing” means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
- “Controller” means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
- “Processor” means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
- “Data Subject” means an individual who is the subject of the relevant personal data.
- “Sensitive Personal Data” or “Special Categories of Personal Data” means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, data concerning health or sex life and sexual orientation, genetic data or biometric data.
“Data Breach” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Other key definitions – please specify (e.g., “Pseudonymous Data”, “Direct Personal Data”, “Indirect Personal Data”)

This is not applicable.

3 Territorial Scope

3.1 Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to those laws?

As expected, Maltese law does not broaden or narrow the territorial scope of the GDPR. In addition, the Data Protection Act and subsidiary legislation enacted under it apply to:

(i) the processing of personal data by a controller or processor established in Malta, regardless of where the processing takes place;
(ii) the processing of personal data of data subjects who are in Malta by a controller or processor not established in the European Union, where the processing activities are related to:
   (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in Malta; or
   (b) the monitoring of their behaviour in so far as their behaviour takes place within Malta; and
(iii) the processing of personal data by a controller not established in the European Union but in a place where the laws of Malta apply by virtue of public international law.

4 Key Principles

4.1 What are the key principles that apply to the processing of personal data?

- **Transparency**
  Personal data must be processed lawfully, fairly and in a transparent manner. Controllers must provide certain minimum information to data subjects regarding the collection and further processing of their personal data. Such information must be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

- **Lawful basis for processing**
  Processing of personal data is lawful only if, and to the extent that, it is permitted under EU data protection law. Article 6(1) of the GDPR provides an exhaustive list of legal bases on which personal data may be processed, of which the following are the most relevant for businesses: (i) prior, freely given, specific, informed and unambiguous consent of the data subject; (ii) contractual necessity (i.e., the processing is necessary for the performance of a contract to which the data subject is a party, or for the purposes of pre-contractual measures taken at the data subject’s request); (iii) compliance with legal obligations (i.e., the controller has a legal obligation, under the laws of the EU or an EU Member State, to perform the relevant processing); or (iv) legitimate interests (i.e., the processing is necessary for the purposes of legitimate interests pursued by the controller, except where the controller’s interest are overridden by the interests, fundamental rights or freedoms of the affected data subjects).

Businesses require stronger grounds to process sensitive personal data (special categories of data). The processing of sensitive personal data is, in accordance with Article 9(2) of the GDPR, only permitted under certain conditions, of which the most relevant for businesses are: (i) explicit consent of the affected data subject; (ii) the processing is necessary in the context of employment law; (iii) the processing is in the vital interest of the data subject or third parties where the data subject is incapable of providing consent; (iv) the data has been publicly revealed by the data subject; or (v) the processing is necessary for the establishment, exercise or defence of legal claims.

- **Purpose limitation**
  Personal data may only be collected for specified, explicit and legitimate purposes and must not be further processed in a manner that is incompatible with those purposes. If a controller wishes to use the relevant personal data in a manner that is incompatible with the purposes for which they were initially collected, it must: (i) inform the data subject of such new processing; and (ii) be able to rely on a lawful basis as set out above.

- **Data minimisation**
  Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which the data is processed. A business should only process the personal data that it actually needs to process in order to achieve its processing purposes.

- **Proportionality**
  The right to protection of personal data is not an absolute right and must be considered in relation to its function in society and be balanced against other fundamental rights in a proportional manner.

- **Retention**
  Personal data must be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

- **Other key principles – please specify**

- **Data Security** – Personal data must be processed in a manner that ensures appropriate security of those data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

- **Accountability** – The controller is responsible for, and must be able to demonstrate, compliance with the data protection principles set out above.

5 Individual Rights

5.1 What are the key rights that individuals have in relation to the processing of their personal data?

- **Right of access to data/copies of data**
  A data subject has the right to obtain from a controller the following information in respect of the data subject’s personal data: (i) confirmation of whether, and where, the controller is processing the data subject’s personal data; (ii) information about the purposes for which the data is being processed; (iii) information about the categories of data being processed; (iv) information about the categories of recipients with whom the data may be shared; (v) information about the period for which the data will be stored (or the criteria used to determine that period); (vi) information about the existence of the rights to erasure, to rectification, to restriction of processing and to object to processing; (vii) information about the existence of the right to complain to the relevant data protection authority; (viii) where the data was not
collected from the data subject, information as to the source of the data; and (ix) information about the existence of, and an explanation of the logic involved in, any automated processing that has a significant effect on the data subject. Additionally, the data subject may request a copy of the personal data being processed.

- **Right to rectification of errors**
  Controllers must ensure that inaccurate or incomplete data is erased or rectified. Data subjects have the right to rectification of inaccurate personal data.

- **Right to deletion/right to be forgotten**
  Data subjects have the right to erase their personal data (the “right to be forgotten”) if: (i) the data is no longer needed for the original purpose (and no new lawful purpose exists); (ii) in the event that the lawful basis for the processing is the data subject’s consent, the data subject withdraws that consent, and no other lawful ground exists; (iii) the data subject exercises the right to object, and the controller has no overriding grounds for continuing the processing; (iv) the data has been processed unlawfully; or (v) erasure is necessary for compliance with EU law or national data protection law. This right is, however, limited in the cases expressly mentioned in Article 17(3) of the GDPR which are related, in the main, to public interest, the freedom of expression and information, legal obligations imposed on the controller to process the data, the exercising of official authority vested in the controller and the establishment, exercise or defence of legal claims.

- **Right to object to processing**
  Data subjects have the right to object, on grounds relating to their particular situation, to the processing of personal data where the basis for that processing is either the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, or the processing is necessary for the purposes of the legitimate interests pursued by the controller. In such a case, the controller must cease such processing unless it demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the relevant data subject or where the processing is required for the establishment, exercise or defence of legal claims.

- **Right to restrict processing**
  Data subjects have the right to restrict the processing of personal data, which means that, with the exception of storage, the data may only be processed by the controller with the data subject’s consent, or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or a Member State if: (i) the accuracy of the data is contested (and only for as long as it takes to verify that accuracy); (ii) the processing is unlawful and the data subject requests restriction (as opposed to exercising the right to erasure); (iii) the controller no longer needs the data for the original purpose, but the data is still required by the controller to establish, exercise or defend legal rights; or (iv) verification of overriding grounds is pending, in the context of an erasure request.

- **Right to data portability**
  Data subjects have a right to receive a copy of their personal data in a commonly used machine-readable format, and transfer their personal data from one controller to another or have the data transmitted directly between controllers.

- **Right to withdraw consent**
  A data subject has the right to withdraw his consent at any time. The withdrawal of consent does not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject must be informed of the right to withdraw consent. It must be as easy to withdraw consent as to give it.

- **Right to object to marketing**
  Data subjects have the right to object to the processing of personal data for the purpose of direct marketing, including profiling.

- **Right to complain to the relevant data protection authority(ies)**
  Data subjects have the right to lodge complaints concerning the processing of their personal data with the IDPC, if the data subjects live in Malta or the alleged infringement occurred in Malta.

### 6 Registration Formalities and Prior Approval

#### 6.1 Is there a legal obligation on businesses to register with or notify the data protection authority(ies) in respect of its processing activities?

The GDPR does away with the general obligation of notifying the supervisory authority (the IDPC) prior to processing personal data. However, Article 7 of the DPA necessitates consultation and prior authorisation with the IDPC where the data controller intends to process, in the public interest:

- genetic data, biometric data or data concerning health for statistical or research purposes; or
- special categories of data in relation to the management of social care services and systems, including for purposes of quality control, management information and the general national supervision and monitoring of such services and systems.

Moreover, in accordance with Article 36 of the GDPR, the IDPC should be consulted where, notwithstanding reasonable mitigating measures taken in terms of available technologies to address high risks following the carrying out of a Data Protection Impact Assessment (“DPIA”), residual risks would still be present.

#### 6.2 If such registration/notification is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?

This is not applicable – please see question 6.1.

#### 6.3 On what basis are registrations/notifications made (e.g., per legal entity, per processing purpose, per data category, per system or database)?

This is not applicable – please see question 6.1.

#### 6.4 Who must register with/notify the data protection authority(ies) for purposes of national data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation?

This is not applicable – please see question 6.1.
### 6.5 What information must be included in the registration/notification (e.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes)?

This is not applicable – please see question 6.1.

### 6.6 What are the sanctions for failure to register/notify where required?

This is not applicable – please see question 6.1.

### 6.7 What is the fee per registration/notification (if applicable)?

This is not applicable – please see question 6.1.

### 6.8 How frequently must registrations/notifications be renewed (if applicable)?

This is not applicable – please see question 6.1.

### 6.9 Is any prior approval required from the data protection regulator?

This is not applicable – please see question 6.1.

### 6.10 Can the registration/notification be completed online?

This is not applicable – please see question 6.1.

### 6.11 Is there a publicly available list of completed registrations/notifications?

This is not applicable – please see question 6.1.

### 6.12 How long does a typical registration/notification process take?

This is not applicable – please see question 6.1.

### 7 Appointment of a Data Protection Officer

#### 7.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.

As per Article 37 of the GDPR, designation of a DPO shall be mandatory where:

- (a) processing is carried out by a public authority or body, except for courts acting in their judicial capacity;
- (b) the core activities of the data controller or processor consist of processing operations which require regular and systematic monitoring of data subjects on a large scale; or
- (c) the core activities of the controller or the processor consist of processing on a large scale of special categories of data and personal data relating to criminal convictions and offences.

#### 7.2 What are the sanctions for failing to appoint a Data Protection Officer where required?

In the circumstances where appointment of a Data Protection Officer is mandatory, failure to comply may result in a wide range of penalties available under the GDPR.

#### 7.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect of his or her role as a Data Protection Officer?

The appointed DPO should not be dismissed or penalised for performing their tasks and should report directly to the highest management level of the controller or processor.

#### 7.4 Can a business appoint a single Data Protection Officer to cover multiple entities?

The appointment of a single DPO covering a group of undertakings is permissible provided that the DPO is easily accessible from each establishment.

#### 7.5 Please describe any specific qualifications for the Data Protection Officer required by law.

The DPO should be appointed on the basis of professional qualities and should have an expert knowledge of data protection law and practices. While this is not strictly defined, it is clear that the level of expertise required will depend on the circumstances. For example, the involvement of large volumes of sensitive personal data will require a higher level of knowledge.

#### 7.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?

A Data Protection Officer should be involved in all issues which relate to the protection of personal data. The GDPR outlines the minimum tasks required by the Data Protection Officer which include: (i) informing the controller, processor and their relevant employees who process data of their obligations under the GDPR; (ii) monitoring compliance with the GDPR, national data protection legislation and internal policies in relation to the processing of personal data including internal audits; (iii) advising on DPIAs and the training of staff; and (iv) co-operating with the data protection authority and acting as the authority’s primary contact point for issues related to data processing.

#### 7.7 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?

Notification to the IDPC will need to be carried out in relation to the appointment of a DPO.

Notification of appointment of a DPO to the IDPC normally entails the provision of the following details:

- Data Controller.
- Name of DPO.
- Position.
- Mailing Address.
7.8 **Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?**

The details of the Data Protection Officer must be published although not necessarily named in the public-facing privacy notice. However, the contact details of the Data Protection Officer must be notified to the data subject when personal data relating to that data subject are collected. As a matter of good practice, the Article 29 Working Party (the “WP29”), today the European Data Protection Board (“EDPB”) recommends that both the data protection authority and employees should be notified of the name and contact details of the Data Protection Officer.

8 **Appointment of Processors**

8.1 **If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?**

Yes. The business that appoints a processor to process personal data on its behalf is required to enter into an agreement with the processor which sets out the subject matter for processing, the duration of processing, the nature and purpose of processing and the obligations and rights of the controller (i.e., the business). It is essential that the processor appointed by the business complies with the GDPR.

8.2 **If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?**

The processor must be appointed under a binding agreement in writing. The contractual terms must stipulate that the processor: (i) only acts on the documented instructions of the controller; (ii) imposes confidentiality obligations on all employees; (iii) ensures the security of personal data that it processes; (iv) abides by the obligations imposed on the controller in relation to the appointment of processors when, in turn, appointing sub-processors; (v) implements measures to assist the controller with guaranteeing the rights of data subjects; (vi) assists the controller in obtaining approval from the Data Protection Officer; (vii) either returns or destroys the personal data at the end of the relationship (except as required by EU or Member State law); and (viii) provides the controller with all information necessary to demonstrate compliance with the GDPR.

9 **Marketing**

9.1 **Please describe any legislative restrictions on the sending of electronic direct marketing (e.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?).**

Data subject consent provided for the purpose of electronic marketing in accordance with Article 6 of the GDPR requires a clear, affirmative act which is given through an active motion or declaration. Moreover, guidance issued by the Article 29 Working Party reiterates that a data subject’s consent cannot be obtained by way of a blanket acceptance of general terms and conditions of a service, for instance. Consequently, prior opt-in consent is required.

This said, where the nature of the goods/services being marketed are such that the data controller may be said to have a legitimate interest in processing a data subject’s personal data, consent will no longer need to be obtained in order to lawfully process said data (for example: where the goods/services marketed are directly linked to the existing relationship between the data controller and the data subject). Moreover, the controller must inform the data subject of his right to object at no cost, to the processing of his personal data for direct marketing purposes.

9.2 **Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.).**

With respect to other means of marketing including unsolicited communications by automated calling machines or fax, the subscriber (both a natural or legal person) must give their prior consent to their personal data being used for direct marketing purposes. In terms of direct marketing carried out by post, consent under the GDPR is understood not to be required, provided that the data controller may prove a legitimate interest in marketing his goods/services.

9.3 **Do the restrictions noted above apply to marketing sent from other jurisdictions?**

Yes, such restrictions apply to marketing sent from other jurisdictions.

9.4 **Is/are the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?**

Yes, the IDPC has dealt with cases involving breaches of marketing restrictions both prior to, and after, the entry into force of the GDPR.

9.5 **Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?**

Yes, it is lawful; however, the entity making such marketing list available should inform the data subjects and obtain their clear and unequivocal consent to the sale of their data by the controller to third parties, prior to such sale taking place. Where the marketing list has been purchased, the information requirements listed in Article 14 of the GDPR would apply.
9.6 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?

Maltese law does not cater for penalties, other than those which may be imposed under the GDPR, in the case of marketing communications that are sent in breach of applicable restrictions.

10 Cookies

10.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).

Currently, Malta implements Article 5 of the ePrivacy Directive (which was transposed into Maltese law by way of the Processing of Personal Data (Electronic Communications Sector) Regulations, S.L. 586.01). Pursuant to Article 5 of the EU ePrivacy Directive, the storage of cookies (or other data) on an end user’s device requires prior consent (the applicable standard of consent is derived from the GDPR). For consent to be valid, it must be informed, specific, freely given and must constitute a real indication of the individual's wishes. This does not apply if: (i) the cookie is for the sole purpose of carrying out the transmission of a communication over an electronic communications network; or (ii) the cookie is strictly necessary to provide an “information society service” (e.g., a service over the internet) requested by the subscriber or user, which means that it must be essential to fulfil their request.

10.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?

Currently, there is no distinction as regards different types of cookies.

10.3 To date, has/have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?

To our knowledge, the IDPC has not taken any enforcement action in relation to cookies as yet.

10.4 What are the maximum penalties for breaches of applicable cookie restrictions?

Maltese law does not cater for penalties, other than those which may be imposed under the GDPR, in the case of breaches of cookie restrictions.

11 Restrictions on International Data Transfers

11.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.

Data transfers to other jurisdictions that are not within the European Economic Area (the “EEA”) can only take place if the transfer is to an “Adequate Jurisdiction” (as specified by the EU Commission) or the business has implemented one of the required safeguards as specified by the GDPR.

Moreover, Article 10 of the DPA stipulates that in the absence of an Adequacy Decision delivered by the EU Commission, the Minister responsible for data protection may, following consultation with the IDPC, by regulations set limits to the transfer of specific categories of personal data to a third country or an international organisation for important reasons of public interest.

11.2 Please describe the mechanisms businesses typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).

When transferring personal data to a country other than an Adequate Jurisdiction, businesses must ensure that there are appropriate safeguards on the data transfer, as prescribed by the GDPR. Some common options include the use of Standard Contractual Clauses or Binding Corporate Rules (“BCRs”).

Businesses can adopt the Standard Contractual Clauses drafted by the EU Commission – these are available for transfers between controllers, and transfers between a controller (as data exporter) and a processor (as data importer). International data transfers may also take place on the basis of contracts agreed between the data exporter and data importer provided that they conform to the protections outlined in the GDPR, and they have prior approval by the relevant data protection authority.

International data transfers within a group of businesses can be safeguarded by the implementation of BCRs. The BCRs will always need approval from the relevant data protection authority. Most importantly, the BCRs will need to include a mechanism to ensure they are legally binding and enforced by every member in the group of businesses. Among other things, the BCRs must set out the group structure of the businesses, the proposed data transfers and their purpose, the rights of data subjects, the mechanisms that will be implemented to ensure compliance with the GDPR and the relevant complainant procedures.

Transfer of personal data to the USA is also possible if the data importer has signed up to the EU-US Privacy Shield Framework, which was designed by the US Department of Commerce and the EU Commission to provide businesses in the EU and the US with a mechanism to comply with data protection requirements when transferring personal data from the EU to the US.

11.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.

In those instances referred to in questions 11.1 and 11.2 above (i.e., (1) where the data importer is established in a EEA Member State, (2) where the data importer is established in a state benefitting from an Adequacy Decision, or (3) where the abovementioned appropriate safeguards are in place to validate the data transfer), notification to the IDPC is not required. Notification to the IDPC is, however, required in any such case where the data transfer not only lacks the measures mentioned above, but also fails to adhere to those conditions set out in Article 49 of the GDPR which allow for derogations in specific situations.

Moreover, as regards Standard Contractual Clauses, authorisation from the IDPC is not required. Conversely, in the case of BCRs,
these must be approved by the IDPC. Alternatively, where appropriate safeguards are adopted in the form of ad hoc contractual clauses or, in the case of public bodies, by means of provisions inserted in administrative arrangements, these must first be authorised by the IDPC.

12 Whistle-blower Hotlines

12.1 What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?

The Protection of the Whistleblower Act, (herein the “PWA”) (Chapter 527 of the Laws of Malta) provides protection to employees in both the private sector and public administration to disclose information regarding improper practices. The term “employee” is defined as:

(a) a person who has entered into or works under a contract of service with an employer, and includes a contractor or subcontractor who performs work or supplies a service or undertakes to perform any work or to supply services;
(b) any person who has undertaken personally to execute any work or service for, and under the immediate direction and control of, another person, including an outworker, but excluding work or service performed in a professional capacity to which an obligation of professional secrecy applies when such work or service is not regulated by a specific contract of service;
(c) any person in employment in the public administration;
(d) any former employee;
(e) any person who is or was seconded to an employer;
(f) any volunteer in terms of law; and
(g) any candidate for employment, but only where information concerning a serious threat to the public interest constituting an improper practice has been acquired during the recruitment process or at another pre-contractual negotiating stage.

The scope of a report made in terms of the PWA is “improper practice”. This term includes an action or series of actions whereby:

(a) a person has failed, is failing or is likely to fail to comply with any law and/or legal obligation to which he is subject;
(b) the health or safety of any individual has been, is being or is likely to be endangered;
(c) the environment has been, is being or is likely to be damaged;
(d) a corrupt practice has occurred or is likely to occur or to have occurred;
(e) a criminal offence has been committed, is being committed or is likely to be committed;
(f) a miscarriage of justice has occurred, is occurring or is likely to occur;
(g) bribery has occurred, is occurring or is likely to occur;
(h) a person acts above his authority; or
(i) information tending to show any matter falling within any one of the preceding paragraphs has been, is being or is likely to be deliberately concealed.

The provisions of the PWA do not apply to members of a disciplined force, members of the Secret Service or persons employed in the foreign, consular or diplomatic service of the Government.

One should also take note of the EDPB (formerly, Article 29 Working Party) Opinion 1/2006 on the application of EU data protection rules to internal whistle-blowing schemes. This is limited to the fields of accounting, internal accounting controls, auditing matters, the fight against bribery, banking and financial crime. The scope of corporate whistle-blower hotlines, however, does not need to be limited to any particular issues. The EDPB recommends that the business responsible for the whistle-blowing scheme should carefully assess whether it might be appropriate to limit the number of persons eligible for reporting alleged misconduct through the whistle-blowing scheme and whether it might be appropriate to limit the number of persons who may be reported through the scheme; in particular, in the light of the seriousness of the alleged offences reported.

12.2 Is anonymous reporting prohibited, strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do businesses typically address this issue?

No, it is not prohibited. However, anonymous reporting is not protected in terms of the PWA. Such an anonymous report may still be taken into account to determine whether an improper practice has occurred. If upon consideration of all circumstances, the report is deemed to be defamatory or libellous, it shall be discarded.

Additionally, anonymous reporting is not prohibited under the GDPR; however, it raises problems as regards the essential requirement that personal data should only be collected fairly. As a rule, the EDPB considers that only identified reports should be advertised in order to satisfy this requirement. Businesses should not encourage or advertise the fact that anonymous reports may be made through a whistle-blower scheme.

An individual who intends to report to a whistle-blowing system should be aware that he/she will not suffer due to his/her action. The whistle-blower, at the time of establishing the first contact with the scheme, should be informed that his/her identity will be kept confidential at all the stages of the process and, in particular, will not be disclosed to third parties, such as the incriminated person or to the employee’s line management. If, despite this information, the person reporting to the scheme still wants to remain anonymous, the report will be accepted into the scheme. Whistle-blowers should be informed that their identity may need to be disclosed to the relevant people involved in any further investigation or subsequent judicial proceedings instigated as a result of any enquiry conducted by the whistle-blowing scheme.

13 CCTV

13.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?

No registration and/or notification to the IDPC is required in this respect. A high-visibility sign would suffice as an adequate form of notice. However, it must be kept in mind that a data protection impact assessment (“DPIA”) should be undertaken with assistance from the DPO when there is a systematic monitoring of a publicly accessible area on a large scale. If the DPIA suggests that the processing would result in a high risk to the rights and freedoms of individuals prior to any action being taken by the controller, the controller must consult the IDPC.

During the course of a consultation, the controller must provide information on the responsibilities of the controller and/or processors involved, the purpose of the intended processing, a copy
of the DPIA, the safeguards provided by the GDPR to protect the rights and freedoms of data subjects and where applicable, the contact details of the Data Protection Officer.

If the data protection authority is of the opinion that the data processing would infringe the GDPR, it has to provide written advice to the controller within eight weeks of the request of a consultation and can use any of its wider investigative, advisory and corrective powers outlined in the GDPR.

13.2 Are there limits on the purposes for which CCTV data may be used?

The use of surveillance cameras must have a clearly defined specific purpose which is proportionate to the rights to privacy of individuals. The IDPC has also issued guidelines as to the use of biometric equipment at the workplace, establishing that this is only permissible in places demanding a high level of security and strict identification procedures.

14 Employee Monitoring

14.1 What types of employee monitoring are permitted (if any), and in what circumstances?

The processing of employee data under GDPR is permitted in so far as it is necessary for the purposes of the employment of the data subject and the processing carried out is proportionate to this need. The processing of employee personal data must be carried out on one of the legal bases listed in Article 6(1) or, in case of sensitive data, Article 9(2) of the GDPR. The Maltese Court of Appeal has recently confirmed that an email address consisting of the name and surname of the employee combined with the IP address of the company with which she was employed, constituted personal data and the employer could not have processed the said personal data by accessing the email account of the employee without giving appropriate notice which, in the circumstances, would have been proportionate to the employer’s needs to access the said personal data.

14.2 Is consent or notice required? Describe how employers typically obtain consent or provide notice.

As mentioned above, processing of an employee’s personal data must be carried out on one of the legal bases provided for in the GDPR. Where the employer needs to rely on “consent” – such as in the case of uploading employee photos on the employer’s website where there is no other ground, such as legitimate interest, for processing the data – the employer must ensure that the employee is informed that the consent should be freely given and that there would be no adverse consequences if he/she were to opt not to provide such consent. Moreover, employees should be informed of the processing activities relating to their data, generally through a privacy policy.

14.3 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?

As regards biometric scanning, the IDPC had established in its past guidance that, where employees are unionised, it is preferable for the employer to consult with the respective union. This is not an obligation under the GDPR and the DPA.

15 Data Security and Data Breach

15.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?

Yes. Personal data must be processed in a way which ensures security and safeguards against unauthorised or unlawful processing, accidental loss, destruction and damage of the data. Both controllers and processors must ensure they have appropriate technical and organisational measures to meet the requirements of the GDPR. Depending on the security risk, this may include: the encryption of personal data; the ability to ensure the ongoing confidentiality, integrity and resilience of processing systems; the ability to restore access to data following a technical or physical incident; and a process for regularly testing and evaluating the technical and organisational measures for ensuring the security of processing.

15.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

The data controller shall be responsible for reporting a personal data breach without undue delay (and in any case within 72 hours of first becoming aware of the breach) to the IDPC, unless the breach is unlikely to result in a risk to the rights and freedoms of the data subject(s). A processor must notify any data breach to the controller without undue delay. The notification must include the nature of the personal data breach, including the categories and number of data subjects concerned, the name and contact details of the Data Protection Officer or relevant point of contact, the likely consequences of the breach, and the measures taken to address the breach, including attempts to mitigate possible adverse effects.

15.3 Is there a legal requirement to report data breaches to affected data subjects? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

Controllers have a legal requirement to communicate the breach to the data subject, without undue delay, if the breach is likely to result in a high risk to the rights and freedoms of the data subject. The notification must include the name and contact details of the Data Protection Officer (or point of contact), the likely consequences of the breach and any measures taken to remedy or mitigate the breach. The controller may be exempt from notifying the data subject if the risk of harm is remote (e.g., because the affected data is encrypted), the controller has taken measures to minimise the risk of harm (e.g., suspending affected accounts) or the notification requires a disproportionate effort (e.g., a public notice of the breach).
15.4 What are the maximum penalties for data security breaches?

The maximum penalty is the higher of €20 million or 4% of worldwide turnover, depending on the nature of the breach. The DPA also makes specific reference to administrative fines on public authorities or bodies, stating that any such fine shall not exceed, in the aggregate: €25,000 for each violation, along with daily fines of €25 for every day during which the violation persists, in relation to violations under Article 83(4) of the GDPR, and €50,000 for each violation, along with daily fines of €50 for every day during which the violation persists, in relation to violations under Article 83(5) or (6) of the GDPR.

16 Enforcement and Sanctions

16.1 Describe the enforcement powers of the data protection authority(ies).

<table>
<thead>
<tr>
<th>Investigatory Power</th>
<th>Civil/Administrative Sanction</th>
<th>Criminal Sanction</th>
</tr>
</thead>
<tbody>
<tr>
<td>Investigative Powers</td>
<td>The data protection authority has wide powers to order the controller and the processor to provide any information it requires for the performance of its tasks, to conduct investigations in the form of data protection audits, to carry out review on certificates issued pursuant to the GDPR, to notify the controller or processor of alleged infringement of the GDPR, to access all personal data and all information necessary for the performance of controllers’ or processors’ tasks and access to the premises of the data including any data processing equipment.</td>
<td>Not applicable.</td>
</tr>
<tr>
<td>Corrective Powers</td>
<td>The IDPC has a wide range of powers, including to issue warnings or reprimands for non-compliance, to order the controller to disclose a personal data breach to the data subject, to impose a permanent or temporary ban on processing, to withdraw a certification and to impose an administrative fine (as below).</td>
<td>Not applicable.</td>
</tr>
<tr>
<td>Authorisation and Advisory Powers</td>
<td>The IDPC has a wide range of powers to advise the controller, accredit certification bodies and to authorise certificates, contractual clauses, administrative arrangements and binding corporate rules as outlined in the GDPR.</td>
<td>Not applicable.</td>
</tr>
<tr>
<td>Imposition of administrative fines for infringements of specified GDPR provisions</td>
<td>The GDPR provides for administrative fines which can be €20 million or up to 4% of the business’ worldwide annual turnover of the preceding financial year. Ad hoc fines for public authorities apply (see details in 15.4, above).</td>
<td>Not applicable.</td>
</tr>
<tr>
<td>Non-compliance with a data protection authority</td>
<td>Not applicable.</td>
<td>The DPA states that without prejudice to the provisions of Articles 21 and 83 of the GDPR, any person who (1) knowingly provides false information to the IDPC when so requested by it pursuant to its investigative powers, or (2) does not comply with any lawful request pursuant to an investigation by the IDPC, shall be guilty of an offence and, on conviction, be liable to a fine (multa) of not less than €1,250 and not more than €50,000 or to imprisonment for six months, or to both such fine (multa) and imprisonment.</td>
</tr>
</tbody>
</table>

16.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?

The GDPR entitles the relevant data protection authority to impose a temporary or definitive limitation, including a ban on processing. A court order is not required.

16.3 Describe the data protection authority’s approach to exercising those powers, with examples of recent cases.

The IDPC tends to scale its approach to enforcement measures depending on the gravity of the breach and the manner in which the controller/processor in question rectifies and responds to the breach. This said, there are no official guidelines or annual reports (post 2011) published by the IDPC.

16.4 Does the data protection authority ever exercise its powers against businesses established in other jurisdictions? If so, how is this enforced?

To our knowledge, the IDPC has, to date, not exercised its powers against businesses established in other jurisdictions although, under the GDPR, it is entitled to do so in those instances in which it would be deemed to be the competent authority.
17 E-discovery / Disclosure to Foreign Law Enforcement Agencies

17.1 How do businesses typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?

Maltese businesses will typically respond to requests for disclosure emanating from public authorities having the power under Maltese law to make such requests. Requests for the provision of information, including personal data, in the context of police investigations could only be made by the executive police under the ordinary Maltese criminal procedures.

17.2 What guidance has/have the data protection authority(ies) issued?

The IDPC has not issued any guidance on this point.

18 Trends and Developments

18.1 What enforcement trends have emerged during the previous 12 months? Describe any relevant case law.

No formal reports are available from the IDPC. We are, however, aware of the fact that the IDPC has been rather active in ensuring compliance with the obligations of the GDPR through various reports being submitted to it, including a number of data breach notifications. In accordance with a February 2019 GDPR Data Breach Survey issued by DLA Piper, it transpires that, until such date, the IDPC had issued approximately 17 fines. This is a significant change to the approach towards enforcement and awareness of data protection obligations in Malta.

18.2 What “hot topics” are currently a focus for the data protection regulator?

No particular trends have emerged.
1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

The legal framework for data protection is found firstly in Articles 6 and 16 of the Mexican Constitution, as well as in the Federal Law for the Protection of Personal Data Held by Private Parties, published in July 2010, and its Regulations, published in December 2011 (hereinafter the “Law”).

1.2 Is there any other general legislation that impacts data protection?

Yes: the General Law for the Protection of Personal Data in the Possession of Obliged Subjects (which regulates the processing of personal information in possession of any Federal, State or local authority); the Privacy Notice Rules, published in January 2013; and the Binding Self-Regulation Parameters, also published in January 2013. It is worth mentioning that Mexican data protection laws and general legislation follow international correlative laws, directives and statutes, and thus have similar principles, regulation scope and provisions.

Moreover, there are other laws such as the Criminal Code, the Law for the Regulation of Credit Information Companies; the Law for Regulating Financing Technology Institutions; provisions set forth in the Copyright Law, the Federal Consumers Law and some specific provisions set forth in the Civil Code and the Commerce Code.

1.3 Is there any sector-specific legislation that impacts data protection?

Mexican data protection legislation is not based on sectoral laws. The Law as described above regulates the collection and processing of any personal information (“PI”) by any private entity acting as a Controller or Processor, which impacts any sector that implies any sort of personal data collection or processing.

1.4 What authority(ies) are responsible for data protection?

The National Institute of Transparency, Access to Information and Personal Data Protection (“INAI”) is the authority responsible for overseeing the Law. Its main purpose is the disclosure of governmental activities, budgets and overall public information, as well as the protection of personal data and the individuals’ right to privacy. The INAI has the authority to conduct investigations; review and sanction data protection Controllers; and authorise, oversee and revoke certifying entities.

The Ministry of Economy is responsible for informing and educating on the obligations regarding the protection of personal data between national and international corporations with commercial activities in Mexican territory. Among other responsibilities, it must issue the relevant guidelines for the content and scope of the Privacy Notice in cooperation with the INAI.

2 Definitions

2.1 Please provide the key definitions used in the relevant legislation:

- **“Personal Data”**
  Any information concerning an individual that may be identified or identifiable.

- **“Processing”**
  The collection, use, disclosure or storage of personal data, by any means. The use covers any action of access, management, benefit, transfer or disposal of personal data.

- **“Controller”**
  The individual or private legal entity that determines the treatment of personal data.

- **“Processor”**
  The individual or legal entity that solely or jointly with another processes personal data on behalf of the Controller.

- **“Data Subject”**
  An identified or identifiable natural person.

- **“Sensitive Personal Data”**
  Personal data which concerns the private life of an individual, or the misuse of such information which may lead to discrimination or carry a serious risk to the individual. In particular, sensitive personal data are considered those that may reveal information such as ethnic or racial origin, a present or future medical condition, genetic information, religious, philosophical and moral beliefs, union affiliation, political opinions and sexual preference.

- **“Data Breach”**
  Data Breach means any security breach which occurred in any phase of the data collection, storage or use, which may affect in a significant manner the patrimonial or moral rights of individuals.
Other key definitions – please specify (e.g., “Pseudonymous Data”, “Direct Personal Data”, “Indirect Personal Data”)

- “ARCO rights”
  Refers to the access, rectification, cancellation or opposition rights to the personal data processing.

- “Consent”
  An expression of will made by the data owner concerning data collection.

- “Pseudonymisation”
  The processing of personal data in such a manner that it can no longer be attributed to a specific data subject without the use of additional information.

- “Privacy Notice”
  A document issued by the Controller either in physical, electronic or in any other format, which is made available to the data subject prior to processing his/her personal data, and whereby the Controller informs the data subject, among others, about: the terms for the collection of personal data; the identity of the Controller; the purpose of the data collection; the possible transfers of data; and the mechanisms for enforcing the ARCO rights.

- “Transfer”
  Any data communication made to a different person other than the Collector or the Processor.

3 Territorial Scope

3.1 Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to those laws?

Businesses located outside Mexico will be subject to the terms of the Privacy Notice, and to the Law, only when the data controller transfers personal data collected in Mexico, in accordance with the provisions of the Law.

4 Key Principles

4.1 What are the key principles that apply to the processing of personal data?

- **Transparency**
  This principle is not defined in the Law; however, the Law also makes clear that personal data can in no way be collected, stored or used through deceitful or fraudulent means.

- **Lawful basis for processing**
  The Collector is responsible for processing personal and/or sensitive data in accordance with the principles set forth in the Law and international treaties.

- **Purpose limitation**
  Personal data shall only be processed for the compliance of the purpose or purposes set forth in the Privacy Notice. Moreover, the purpose of the Privacy Notice must be certain, which is achieved by establishing the purpose for which the personal data will be processed in a clear, objective manner, not giving room for confusion.

- **Data minimisation**
  The Collector will be responsible and shall endeavour to make reasonable efforts so that the personal data processed are of the minimum necessary, according to the purpose that originated the collection of PI.

- **Proportionality**
  Data controllers can only collect personal data that are necessary, appropriate and relevant for the purpose(s) of the collection.

- **Retention**
  This translates into the obligation of the Collector to retain personal data only for the period of time necessary for complying with the purpose(s) for which the data was collected, with the obligation to block, cancel and suppress the personal data afterwards.

Other key principles – please specify

- “Responsibility”
  The Collector must safeguard and be accountable of any PI under its custody, or any PI that it has shared with any vendor, either in Mexico or abroad. In order to comply with this principle, the Controller must make use of any of the best international practices, corporate policies, self-regulatory schemes or any other suitable mechanism for this effect.

- **“Quality”**
  This principle is accomplished when personal data processed are accurate, complete, pertinent, correct and updated as required, in order to comply with the purpose for which the personal data will be collected.

- **“Consent”**
  The Controller shall obtain the consent of the data subject, in advance, with the aim of processing any PI, and must keep evidence of the consent.

- **“Loyalty”**
  This consists of the obligation of the data controller to process any PI collected favouring the protection of the interests of the data subject and the reasonable expectation of privacy.

5 Individual Rights

5.1 What are the key rights that individuals have in relation to the processing of their personal data?

- **Right of access to data/copies of data**
  Data subjects have the right to access their personal data held by the data controller at any time they request.

- **Right to rectification of errors**
  Data subjects have the right to request the rectification of any of their personal data held by a data controller, if it is inaccurate, incomplete or dated.

- **Right to deletion/right to be forgotten**
  Data subjects have the right to request the cancellation of their personal data. The cancellation of personal data will result in a blocking period after which the suppression of the data will take place. Notwithstanding the foregoing, the data controller may keep such personal data exclusively for the purposes of the responsibilities regarding the treatment. Likewise, the Law establishes some cases where the data controller is not obliged to cancel or delete the personal data.

- **Right to object to processing**
  Data owners have the right to object to the processing of their personal data due to a legitimate reason.

- **Right to restrict processing**
  Data owners have the right to restrict the processing of their personal data due to a legitimate reason.

- **Right to data portability**
  The data owner has the right to obtain from the obliged subject a copy of his/her processed data, which allows the data subject to continue using his/her personal information.
Right to withdraw consent
At any time, the data owner may withdraw his/her consent for the treatment of his/her personal data, for which the data controller must establish simple and free mechanisms which allow the data subjects to withdraw their consent at least by the same means by which they granted it.

Right to object to marketing
In addition to the general rights described above, data owners have the right to oppose the use of their personal data for marketing or advertising purposes.

Right to complain to the relevant data protection authority(ies)
Data owners are entitled to submit a claim before the INAI. The claim must be filed in writing and shall clearly state the provisions of the Law that are deemed infringed; also, it must be submitted within the 15 days following the date on which the response to the data owner has been communicated by the data controller.

Other key rights – please specify
Right to a verification procedure
Data subjects will have the right to request before the data protection authority (“DPA”), a verification procedure, in which the authority will check the data controller’s compliance with all the provisions set forth in the Law, or any other applicable regulations.

6 Registration Formalities and Prior Approval

6.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?

No, there is not.

6.2 If such registration/notice is needed, must it be specific (e.g., listing all processing activities, categories of data, etc) or can it be general (e.g., providing a broad description of the relevant processing activities)?

This is not applicable.

6.3 On what basis are registrations/notifications made (e.g., per legal entity, per processing purpose, per data category, per system or database)?

This is not applicable.

6.4 Who must register with/notify the data protection authority (e.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation)?

This is not applicable.

6.5 What information must be included in the registration/notification (e.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes)?

This is not applicable.

6.6 What are the sanctions for failure to register/notify where required?

This is not applicable.

6.7 What is the fee per registration/notification (if applicable)?

This is not applicable.

6.8 How frequently must registrations/notifications be renewed (if applicable)?

This is not applicable.

6.9 Is any prior approval required from the data protection regulator?

This is not applicable.

6.10 Can the registration/notification be completed online?

This is not applicable.

6.11 Is there a publicly available list of completed registrations/notifications?

This is not applicable.

6.12 How long does a typical registration/notification process take?

This is not applicable.

7 Appointment of a Data Protection Officer

7.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.

Yes, the appointment of a Data Protection Officer (person or department) by the Controller is mandatory.

7.2 What are the sanctions for failing to appoint a Data Protection Officer where required?

The failure in appointing the Data Protection Officer (person or department) is not expressly regulated as an infringement yet.
7.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect of his or her role as a Data Protection Officer?

No, they are not.

7.4 Can a business appoint a single Data Protection Officer to cover multiple entities?

Yes, they can.

7.5 Please describe any specific qualifications for the Data Protection Officer required by law.

There are no statutory requirements. Notwithstanding the foregoing, it is recommended to appoint a person or department at least with the following qualifications: i) data privacy expertise; and ii) enough authority and resources to implement measures in order to protect the personal data.

7.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?

The responsibilities of a Data Protection Officer required by law are to: i) process all claims related to the enforcement of the ARCO rights; and ii) foster and enhance the protection of personal data inside the company.

7.7 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?

No, there is no statutory obligation to register or notify the appointment of a Data Protection Officer to any authority.

7.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?

No, it is not mandatory to appoint a Data Protection Officer, being only necessary to mention in the Privacy Notice the name and domicile of the person or department that will be responsible for the collection, use and storage of the personal data.

8 Appointment of Processors

8.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?

Yes, the relationship between the business and the Processor must be established by means of contractual clauses or other legal instruments determined by the business; and it is necessary to prove the existence, scope and content of the relationship.

8.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?

The agreement shall be in writing and signed by both parties. The agreement shall contain at least the following obligations for the Processor: i) to treat only personal data according to the instructions of the business; ii) to treat only personal data for the purposes instructed by the business; iii) to implement security measures in accordance with the Law, and other applicable provisions; iv) to keep confidentiality regarding the personal data processed; v) to delete all PI processed once the legal relationship with the business is over, or when the instructions of the business have been fulfilled, provided that there is no legal provision that requires the preservation of the personal data; and vi) to refrain from transferring PI unless the business determines so, or when it is required by a competent authority. It is worth mentioning that the agreements between the business and the Processor related to the treatment of the personal data must be in accordance with the corresponding Privacy Notice.

9 Marketing

9.1 Please describe any legislative restrictions on the sending of electronic direct marketing (e.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?).

Mexico does not have any specific regulation dealing with unsolicited text messages or spam emails, but the Federal Bureau for Consumer Protection operates a call blocking registry, called REPEP, covering both landlines and mobile phone numbers, which gives suppliers 30 days to stop making marketing calls, sending marketing messages and to stop disturbing the consumer at his/her registered address, electronic address, or by any other means.

9.2 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.).

Please refer to question 9.1 above.

9.3 Do the restrictions noted above apply to marketing sent from other jurisdictions?

Please refer to question 9.1 above.

9.4 Is/are the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?

Issues regarding marketing restrictions are regularly addressed by the Federal Bureau for Consumer Protection.

9.5 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?

Yes, but in the Privacy Notice the Controller must provide detailed information as to the data transfers that it is willing to make,
involving PI, expressly indicating the name of the data processor(s), of the type, category of activity sector of the latter; and expressly indicating the purpose(s) of such transfer(s). Also, when required, a clause indicating whether or not the data subject consents to the data transfer should be included.

9.6 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?

According to the Federal Consumer Protection Law, the maximum penalties for marketing breaches may reach the amount of MXN$1,317,141.34 (approximately US$70,000).

10 Cookies

10.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).

Yes. The Guidelines for elaborating the Privacy Notice require that individuals are informed as to any technology that allows the automatic collection of PI simultaneously to the first contact with the individuals; requiring data owners to request the consent from individuals through an opt-in mechanism, and informing individuals as to how to deactivate said technology, unless said technology is required for technical reasons.

10.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?

No, they do not.

10.3 To date, has/have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?

No, they have not.

10.4 What are the maximum penalties for breaches of applicable cookie restrictions?

Although there is not any express infringement regulated in the Law in connection with the use of cookies, their use in contravention to the Guidelines mentioned above would translate to an illicit collecting of PI, which would be sanctioned with fines of up to US$680,000, and if the infringement persists, additional fines of up to US$1,300,000 may be imposed.

11 Restrictions on International Data Transfers

11.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.

If the Controller is willing to transfer any PI to any third parties, either domestic or foreign, it needs to obtain the informed consent of data subjects for the said data transfer, in advance, through the Privacy Notice. There are some cases where third parties do not require the consent of the data subject for the transfer of PI. According to Article 37 of the FLPPIPPE, consent will not be necessary only in the following cases:

i) when expressly allowed by the Law;
ii) when PI is available in public access sources;
iii) when personal data has been dissociated;
iv) when the collection of personal data is needed for compliance with obligations derived from a legal relationship between the data subject and the data owner;
v) when there is an emergency situation that jeopardises the person or the commodities of the data subject; and
vi) when the collection of PI is indispensable for medical attention and/or diagnosis; for rendering sanitary assistance; for medical treatment or sanitary services; provided that the data subject is not in a condition to give consent; and provided that the data collection is performed by a person subject to legal professional privilege.

11.2 Please describe the mechanisms businesses typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).

As stated above, according to Article 36 of the FLPPIPPE, if any Controller is willing to transfer any PI to third parties, either domestic or foreign, it must obtain consent from the data subject in advance, through a Privacy Notice. When the transfer is performed, the vendor or third party will be obliged exactly in the same terms as the Controller.

11.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.

There is no registration/notification requirement set forth in the Law for data transfers.

12 Whistle-blower Hotlines

12.1 What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?

Whistle-blower hotlines can be set into operation, but the Law is silent as to any restrictions on the personal data that may be processed through them.

12.2 Is anonymous reporting prohibited, strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do businesses typically address this issue?

Anonymous and non-anonymous reporting is allowed.
13 CCTV

13.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?

There is no registration or notification requirement for the use of CCTV.

13.2 Are there limits on the purposes for which CCTV data may be used?

The Law is silent as to the limits on the purposes for which CCTV data may be used.

14 Employee Monitoring

14.1 What types of employee monitoring are permitted (if any), and in what circumstances?

Mexican legislation is silent as to the types of employee monitoring that are permitted and the circumstances under which said monitoring is allowed.

Therefore, the balance between the monitoring that can be made by employers and the respect of the privacy of employees is to be found in the general rules set forth in Articles 6 and 16 of the Mexican Constitution, which regulates the right to privacy, and the general rules established by the legislation on Data Privacy. These rules should be interpreted by the Mexican Courts on a case-by-case basis, in order to generate jurisprudence in this regard.

For instance, video surveillance of public spaces in workplaces is allowed, while surveillance at restrooms and locker rooms is prohibited.

Monitoring phone calls made by employees is allowed, but only to determine the user of the phone call and the length of the call, and not the content of the call.

14.2 Is consent or notice required? Describe how employers typically obtain consent or provide notice.

Since the collection, storage and use of any audio or video material featuring the voice and image of any individual within the workplace may be deemed as a collection of PI, employers would be required to give employees notice as to the use of video surveillance technology at workplaces.

The Mexican DPA has drawn up a model short Privacy Notice to be used by any individual or company introducing video surveillance technology on their premises.

Said summary Privacy Notice must be visible at the entrance of the monitored spaces, and must inform individuals of the purpose of the surveillance, and the treatment of the collected information.

14.3 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?

Employee representatives at councils/trade unions do not need to be either consulted or notified.

15 Data Security and Data Breach

15.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?

Article 19 of the Federal Law for the Protection of Personal Information in Possession of Private Entities requires every data controller to implement and maintain administrative, technical and physical security measures, which prevent the collected and stored PI from any loss, alteration, destruction or from any unauthorised access and use.

Said measures cannot be lesser than those used by the data owner to protect its own information, and for its implementation the data owner must consider the existing risk and the possible consequences for the data subjects, the sensitivity of the data and the technological development.

15.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

There is no legal requirement to report data breaches to the Mexican DPA, and so far, there are no guidelines for voluntary breach reporting to the Mexican DPA.

15.3 Is there a legal requirement to report data breaches to affected data subjects? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

If any phase of the data collection, storage or use may in any way affect in a significant manner the patrimonial or moral rights of individuals, data owners shall immediately notify individuals about this situation.

Likewise, Article 64 of the Regulations of the FLPPIPPE requires data owners to notify individuals without any delay as to any breach that significantly affects their moral or patrimonial rights, as soon as the data owner confirms that a breach has occurred, and when the data owner has taken any actions towards starting an exhaustive process to determine the magnitude of the breach.

In said notification, data owners must state at least:

- the nature of the incident;
- the compromised PI;
- recommendations for the data subjects to protect their interests;
- the corrective measures immediately implemented by the data owner; and
- the means for getting more information regarding the breach.

15.4 What are the maximum penalties for data security breaches?

According to the Federal Consumer Protection Law, the penalties for data security breaches regarding marketing matters range from MXN$260.56 to MXN$833,823.71.
On the other hand, the Mexican DPA (INAI) is entitled to impose administrative sanctions such as fines of up to MXN$25,000,000 (approximately USD$1,400,000).

Additionally, there are two activities deemed as felonies related to the wrong use of PI, which are:

i) When a data owner authorised to collect, store and use PI with the aim of profiting, causes a security breach in the database containing PI under its custody. This is sanctioned with imprisonment from three months to three years.

ii) To collect, use or store PI, with the aim of profiting, through error or deceit of the data subject, or error or deceit of the person who has to authorise the transfer. This is sanctioned with imprisonment from six months to five years.

16 Enforcement and Sanctions

16.1 Describe the enforcement powers of the data protection authority(ies).

<table>
<thead>
<tr>
<th>Investigatory Power</th>
<th>Civil/Administrative Sanction</th>
<th>Criminal Sanction</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Mexican DPA (INAI) is entitled to conduct visits of inspection ex officio to any company, in order to determine the compliance to the legislation on PI. The INAI is also entitled to prosecute and resolve any complaint tending to enforce the ARCO rights of any individual.</td>
<td>The Mexican DPA is not entitled to declare damages, thus it is necessary to file an independent civil action before the Mexican Civil Courts for that effect.</td>
<td>As stated above, the FLPPPIPE provides some criminal sanctions if there is an intention to profit from the security breach of PI. However, the Mexican DPA is not entitled to prosecute criminal actions, thus it is necessary to file the corresponding criminal complaint before the Attorney General’s Office, and the criminal action will be decided by a Criminal Court.</td>
</tr>
<tr>
<td>Not applicable.</td>
<td>The administrative infringements set forth in the FLPPPIPE are prosecuted before the INAI, and the ruling that this DPA issues can further be appealed before the Federal Court for Administrative Affairs. The decision that this Court gets to issue can further be appealed through a constitutional rights action, known as Amparo, before the Federal Circuit Courts.</td>
<td>Not applicable.</td>
</tr>
</tbody>
</table>

16.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?

This authority is not expressly recognised in the Law in favour of the INAI. However, considering that the FLPPPIPE recognises the INAI as the specialised authority in charge of the protection of PI in Mexico, the INAI should be deemed as having the authority to ban a particular processing activity. However, if contested by any third party, any ban issued by the INAI should be validated by Mexican Federal Administrative Courts.

16.3 Describe the data protection authority’s approach to exercising those powers, with examples of recent cases.

So far there are no recent cases or precedents illustrating this authority’s approach.

16.4 Does the data protection authority ever exercise its powers against businesses established in other jurisdictions? If so, how is this enforced?

Please refer to question 16.1 above.

17 E-discovery / Disclosure to Foreign Law Enforcement Agencies

17.1 How do businesses typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?

Any e-discovery requests or requests for disclosure from foreign law enforcement agencies have to be validated by Mexican Courts, so that they can be validly enforced in Mexico. If any order or request from any foreign law enforcement agency is not validated through a Mexican Court, a company may refuse to comply with it.

17.2 What guidance has/have the data protection authority(ies) issued?

In connection with e-discovery and disclosure to foreign law enforcement agencies, no guidance has been issued by the Mexican DPA.

18 Trends and Developments

18.1 What enforcement trends have emerged during the previous 12 months? Describe any relevant case law.

There are no trends which have emerged during the previous 12 months.
However, at the time of writing this article, as a result of an investigation process started by the Mexican DPA (INAI), in February 2019, related to a data breach at KPMG Mexico, INAI is raising its voice as to the need to modify Mexican data protection law, in order to include an obligation to notify the DPA in case of a data breach.

18.2 What “hot topics” are currently a focus for the data protection regulator?

In June 2018, Mexico joined the Convention for the protection of individuals with regard to automatic processing of personal data (Convention 108), and the additional protocol to Convention 108 regarding supervisory authorities and transborder data flows (ETS No. 181). This constitutes a very important step for Mexico towards the enhancement of personal information, since these documents bind Mexico into carrying out the automatic processing of personal information, in accordance to European standards. At the same time, this provides international tools that will enhance trans-border data flows, which should trigger foreign investment into Mexico.

A lot of buzz was also created by the entering into force of the GDPR in May 2018, which posed the question to many Mexican companies, as to whether or not there was something additional to be done in order to comply with the GDPR, as well as complying with domestic privacy law.

Abraham Diaz Arceo co-chairs the Privacy and IT Industry group and has a wealth of knowledge across the IP spectrum. Abraham focuses his practice on copyright, trademarks and unfair competition, litigation, licensing and prosecution matters. He counsels clients on any IP-related matters, and handles matters involving trademarks, trade dress, product configuration, unfair competition, advertisement-related matters, false advertising, trade secrets, plant breeders' rights, vegetal varieties and Internet-related IP issues. His Internet experience includes handling domain disputes under the UDRP, as well as counselling clients concerning the development of websites and the protection of the content thereof. He also counsels clients with regards to the correct implementation, monitoring and auditing of privacy management programmes, and crisis and data breach management.

Because of his broad background, Mr. Diaz is perfectly placed to advise clients on a range of subjects and is able to assess the legal needs within this sector from a 360° standpoint.

Gustavo A. Alcocer joined OLIVARES as a Partner in 1999. He manages the Corporate and Commercial Law Group and is Co-Chair of the Life Sciences and Pharmaceuticals Group. Prior to joining OLIVARES, he acted as In-House Counsel for Banamex for 11 years in various positions, including Vice-President of International Legal Affairs in New York and Executive Vice-President and Assistant General Counsel for Grupo Financiero Banamex in Mexico City.

Mr. Alcocer possesses a wealth of transactional experience in M&A, finance and business law and advises our clients on complex M&A, finance, asset sale and acquisition, licensing, franchising, real estate transactional work and regulatory work. Clients routinely turn to him for sophisticated strategic advice regarding structuring, maintaining and expanding operations in Mexico and IP valuation and monetisation. Additionally, Mr. Alcocer has worked with international companies in FCPA and anti-bribery compliance, as well as privacy and personal data protection.
1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

In Niger, the processing of personal data is governed by Law no. 2017-28 of 3 May 2017 relating to the protection of personal data (the Personal Data Law – PDL).

1.2 Is there any other general legislation that impacts data protection?

No, there is no other legislation that impacts data protection.

1.3 Is there any sector-specific legislation that impacts data protection?

No, there is no sector-specific legislation.

1.4 What authority(ies) are responsible for data protection?

The authority responsible for the protection of personal data is the High Authority for the Protection of Personal Data (HAPD), whose powers are governed by Law no. 2017-28 of 3 May 2017.

2 Definitions

2.1 Please provide the key definitions used in the relevant legislation:

- **“Personal Data”**
  Any information of any kind and regardless of its medium, including sound and image, and relating to a natural person identified or identifiable directly or indirectly, by reference to an identification number or to several elements specific to its physical, physiological, genetic, psychological, cultural, social or economic identity.

- **“Processing”**
  Processing of personal data means any operation or set of operations in relation to such data, especially its collection, exploitation, registration, organisation, storage, adaptation, modification, retrieval, backup, copying, consultation, disclosure by transmission, dissemination or otherwise making available, alignment, locking, encryption, erasure or destruction.

- **“Controller”**
  Any person who has authority over the processing of personal data.

- **“Processor”**
  A natural or legal person, whether public or private, or any other body or association which, alone or jointly with others, decides to collect and process personal data and determines its purpose.

- **“Data Subject”**
  Any individual person whose personal data are processed.

- **“Sensitive Personal Data”**
  Any information of any kind and regardless of its medium, including sound and image, and relating to a natural person identified or identifiable directly or indirectly, by reference to an identification number or to several elements specific to its physical, physiological, genetic, psychological, cultural, social or economic identity.

- **“Data Breach”**
  Any operation or attempted operation on such data, especially its interception, misappropriation, damage, deletion, erasure, alteration, counterfeiting by an unauthorised production, use, backup or transfer process.

- **Other key definitions – please specify (e.g., “Pseudonymous Data”, “Direct Personal Data”, “Indirect Personal Data”).**
  There are no other specific key definitions.

3 Territorial Scope

3.1 Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to those laws?

Yes. These laws are applicable where the business relationship or business activity is based in the Republic of Niger.
4 Key Principles

4.1 What are the key principles that apply to the processing of personal data?

- **Transparency**
  Article 18 of the PDL requires clear and prior information to be provided by any person responsible for the collection and processing of the data.

- **Lawful basis for processing**
  Under Articles 14 and 15 of the PDL, data must be processed legally and lawfully.

- **Purpose limitation**
  The retention of the processed data may not exceed a time limit for its purposes, as provided for in Article 16 of the PDL.

- **Data minimisation**
  Article 16 requires that personal data must be used only for the purpose for which they were collected.

- **Proportionality**
  Refer to “data minimisation”.

- **Retention**
  Article 16 of the PDL requires that the retention of personal data may not exceed their time limit for use, unless they are used for research, historical or statistical purposes.

- **Other key principles – please specify**
  **Confidentiality**
  According to Article 19 of the PDL, the data must be treated confidentially and protected. However, the rights of persons whose data are processed are derogated in the case of the exercise of the right to freedom of expression, for grounds of general interest in the field of public health, for compliance with the law, and in the event of an obligation on the controller to keep the data.

5 Individual Rights

5.1 What are the key rights that individuals have in relation to the processing of their personal data?

- **Right of access to data/copies of data**
  Article 26 of the PDL gives obligation to the processor to allow the individuals to have access to their personal data.

- **Right to rectification of errors**
  Article 29 of the PDL allows the individual to require rectification towards the processor.

- **Right to deletion/right to be forgotten**
  Article 30 also allows individuals who inherit from deceased persons to delete and update the personal data used.

- **Right to object to processing**
  Article 26, point 5 gives the individual this right; Article 28 also defines the right for him to prohibit any use of his personal data that contravenes his rights.

- **Right to restrict processing**
  Article 28 of the PDL allows the individual to require restriction on the part of the processor.

- **Right to data portability**
  There is no specific article in this regard.

- **Right to withdraw consent**
  Article 28 also defines the rights for him to prohibit any use of his personal data that contravenes his rights.

- **Right to object to marketing**
  There is no specific article but in a global sense these rights are defined by Article 28 of the PDL.

- **Right to complain to the relevant data protection authority(ies)**
  Article 51 of the PDL allows the individual to request any kind of information from the data protection authority.

Other key rights – please specify

6 Registration Formalities and Prior Approval

6.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?

Article 5 of the DPA requires establishments processing personal data to first make a declaration to the Personal Data Protection Authority.

6.2 If such registration/notice is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?

The statement is specific.

6.3 On what basis are registrations/notifications made (e.g., per legal entity, per processing purpose, per data category, per system or database)?

Statements are made in accordance with the purpose of the processing.

6.4 Who must register with/notify the data protection authority (e.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation)?

According to Article 7 of the HPA, the declaration is made by the controller or his legal representative.

6.5 What information must be included in the registration/notification (e.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes)?

According to the provisions of Article 9, the application for authorisation or declaration must contain:

- all information relating to the identity, domicile and mailing address of the controller and his legal representative;
- the purpose of the processing and the general description of its functions;
the interconnections envisaged, as well as all forms of linking with other treatments;
- the data processed, their origin and the categories of persons concerned;
- the duration of retention of processed data;
- the departments responsible for implementing the processing;
- the recipients entitled to receive data communication;
- the function of the person or service for which the right of access to data is exercised; and
- arrangements made for the security and confidentiality of processed data.

6.6 What are the sanctions for failure to register/notify where required?

In the event of non-reporting, the Authority may, in accordance with Article 54 of the HPA:
- interrupt the implementation of the processing;
- lock certain personal data; and
- prohibit temporary or permanent treatment contrary to the provisions of the law.

6.7 What is the fee per registration/notification (if applicable)?

There are no fees.

6.8 How frequently must registrations/notifications be renewed (if applicable)?

The registrations are made only once.

6.9 Is any prior approval required from the data protection regulator?

Under Article 7 of the HPA, prior authorisation is required in the case of:
- treatment of genetic, medical and scientific data in these areas;
- processing of data on offences, convictions and security measures;
- processing of a national identification number or any other identifier of the same nature;
- processing of biometric data;
- processing of data of public interest; or
- processing of data intended for a third country.

6.10 Can the registration/notification be completed online?

Reporting can be done online, as per section 10 of the HPA.

6.11 Is there a publicly available list of completed registrations/notifications?

To our knowledge, there is no such list.

6.12 How long does a typical registration/notification process take?

Upon receipt of the application for authorisation or the declaration, the Authority shall have one month to respond. This period may be extended only once for the same period (Article 11 PDL).

7 Appointment of a Data Protection Officer

7.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.

Article 9 of the PDL does not require the controller to appoint a personal data protection officer. However, it states that in the declaration or application for authorisation, the service or persons having access to treatment must be mentioned.

7.2 What are the sanctions for failing to appoint a Data Protection Officer where required?

The law makes no mention of any sanction.

7.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect of his or her role as a Data Protection Officer?

The officer in charge of protection has no special immunity.

7.4 Can a business appoint a single Data Protection Officer to cover multiple entities?

The law does not provide for any limitation of the duties of the protection officer.

7.5 Please describe any specific qualifications for the Data Protection Officer required by law.

The law does not provide for any particular qualification.

7.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?

The law on the protection of personal data in force in Niger does not stipulate any responsibility.

7.7 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?

The law does not require specific notification to be made to the HAPD as to the appointment of a data protection officer.

7.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?

The law does not mention any conditions relating to the appointment of the data protection officer.
8 Appointment of Processors

8.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?

The business shall sign a subcontracting agreement with the processor.

8.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?

The PDL does not define any specific formalities or issues.

9 Marketing

9.1 Please describe any legislative restrictions on the sending of electronic direct marketing (e.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?).

The PDL has not defined any restrictions.

9.2 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.).

The PDL has not defined any restrictions.

9.3 Do the restrictions noted above apply to marketing sent from other jurisdictions?

This is not applicable.

9.4 Is/are the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?

This is not applicable.

9.5 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?

No, this is not permitted.

9.6 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?

There are no maximum penalties.

10 Cookies

10.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).

There is no provision in our jurisdiction relating to cookies and their use.

10.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?

No, this is not applicable in Niger.

10.3 To date, has/have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?

No, this is not applicable in Niger.

10.4 What are the maximum penalties for breaches of applicable cookie restrictions?

This is not applicable in Niger.

11 Restrictions on International Data Transfers

11.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.

The PDL does not stipulate any kind of restriction.

11.2 Please describe the mechanisms businesses typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).

There are no particular mechanisms.

11.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.

There are no specific practical approvals required.

12 Whistle-blower Hotlines

12.1 What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?

The PDL does not set any kind of scope in this regard.
12.2 Is anonymous reporting prohibited, strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do businesses typically address this issue?

This is not applicable in Niger.

13 CCTV

13.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?

No, in fact there are no specific rules relating to CCTV.

13.2 Are there limits on the purposes for which CCTV data may be used?

No, due to the lack of regulation.

14 Employee Monitoring

14.1 What types of employee monitoring are permitted (if any), and in what circumstances?

No specific types of monitoring are defined.

14.2 Is consent or notice required? Describe how employers typically obtain consent or provide notice.

No specific types of monitoring are defined.

14.3 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?

Such consultation is not required.

15 Data Security and Data Breach

15.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?

Articles 38 and 39 of the PDL require the processor to ensure the security of personal data that they use.

15.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

There is no legal requirement.

16 Enforcement and Sanctions

16.1 Describe the enforcement powers of the data protection authority(ies).

This is not applicable in Niger.

16.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?

The Authority has the power to inform the court of activities falling under Article 51 of the PDL.

16.3 Describe the data protection authority’s approach to exercising those powers, with examples of recent cases.

There are no examples available, as the Authority is not yet functioning.

16.4 Does the data protection authority ever exercise its powers against businesses established in other jurisdictions? If so, how is this enforced?

No, as the Authority is not yet functioning.

17 E-discovery / Disclosure to Foreign Law Enforcement Agencies

17.1 How do businesses typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?

There is no typical response on the part of businesses.

17.2 What guidance has/have the data protection authority(ies) issued?

No guidance has been issued.
18  Trends and Developments

18.1 What enforcement trends have emerged during the previous 12 months? Describe any relevant case law.

There are no trends to report, as data protection is still an emerging area of practice in our jurisdiction.

18.2 What “hot topics” are currently a focus for the data protection regulator?

There are no current topics of particular note.
Nigeria

Infusion Lawyers

Chapter 34

1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

Nigeria does not have a principal data protection law. However, Nigeria has subsidiary data protection legislation: the Nigeria Data Protection Regulation 2019 (‘the Regulation’). This Regulation was issued by the National Information Technology Development Agency (NITDA) on 25 January 2019. It is made by virtue of the National Information Technology Development Act (NITDA Act 2007), the principal Act. By virtue of section 32 of the NITDA Act 2007, NITDA is responsible for making “regulations it deems necessary or expedient for giving full effect to the provisions of the NITDA Act and for effective administration of its provisions”. The Regulation repealed the Data Protection Guidelines 2013 (‘the Guidelines’).

Apart from the Regulation, Nigeria has provisions on data protection in various pieces of legislation and regulations, across a number of industries and sectors.

1.2 Is there any other general legislation that impacts data protection?

- The 1999 Constitution of the Federal Republic of Nigeria (as amended): The Nigerian Constitution, under section 37, guarantees citizens’ privacy as a fundamental human right. It protects citizens’ homes, correspondence, telephone conversations, and telegraphic communications. But privacy as a constitutional right may be validly restricted as long as it is “reasonably justifiable in a democratic society (a) in the interest of defence, public safety, public order, public morality or public health; or (b) for the purpose of protecting the rights and freedom or other persons” (section 45 of the Constitution).

- The Freedom of Information Act 2011: The Freedom of Information Act is not a data protection law, but section 14 of the Act protects personal data. Since the Act governs access to public records and information in Nigeria, the section restricts disclosure of personal records without obtaining consent.

- The Nigerian Communications Act 2003: By virtue of the powers conferred by the NCA 2003 on the Nigerian Communications Commission (NCC), regulations that touch on data protection in the telecommunications industry have been made by NCC. These regulations are the General Consumer Code of Practice Regulation, the Registration of Telephone Subscribers Regulations (‘RTS Regulation’) 2011, and the Nigerian Communications ( Enforcement Process, etc.) Regulation 2005.

- The Child Rights Act 2003: The Act reinforces the constitutional rights of the child, including privacy rights under section 37 of the 1999 Constitution. Under section 8 of the Act, the Nigerian child’s right to privacy, family life, home, correspondence, telephone conversation, and telegraphic communications are protected.

- The Cybercrimes (Prohibition, Prevention, etc.) Act 2015 (Cybercrimes Act): Under the Cybercrimes Act, abuse and misuse of data for fraudulent purposes are criminalised. Service providers have a duty of record retention and data protection. They are to keep all traffic data and subscriber information for a period of two years.

- The National Identity Management Commission Act 2007 (NIMC Act): By virtue of section 31 of the NIMC Act, the National Identity Management Commission (NIMC) makes regulations for the effective operation of the Act. NIMC’s powers include the power to provide for the collection, collation, and processing of data and any other relevant information.

1.3 Is there any sector-specific legislation that impacts data protection?

- The Consumer Code of Practice Regulations 2007: In the telecommunications sector, the Code applies to telecom service providers in Nigeria. The Code governs licensed telecommunications operators in Nigeria and related consumer practices.

- Nigerian Communications Commission (Registration of Telephone Subscribers) Regulations 2011 (RTS Regulation): Also in the telecommunications sector, it protects data privacy and confidentiality of subscribers’ personal data. Collection, collation, management, and storage of subscribers’ personal data are regulated.

- Consumer Protection Framework (the “Framework”) 2016: In the financial sector, the Central Bank of Nigeria (CBN) introduced the Consumer Protection Framework. One of the provisions of this Act is that it protects consumer assets and privacy.

- The Credit Reporting Act 2017: In the financial sector, the Credit Reporting Act promotes access to credit information. Amongst other things, it protects the confidentiality rights of data subjects, including the right to consent and the right to accurate personal information.

- The National Health Act 2014: In Nigeria’s health sector, the National Health Act requires health service providers to keep a record of patients’ personal information by storing every user’s health records safely and in strict confidentiality.
1.4 What authority(ies) are responsible for data protection?

There is no single data protection authority in Nigeria. Under each principal and subsidiary piece of legislation – either general or sector-specific – there are different authorities responsible for data protection:

- **National Information Technology Development Agency (NITDA):** NITDA issued the Nigeria Data Protection Regulation 2019 and the agency is a data protection authority under the Regulation.
- **Nigerian Communications Commission (NCC):** NCC is the data protection authority under the General Consumer Code of Practice for Telecommunications, the Registration of Telephone Subscribers Regulation (‘RTS Regulation’) 2011, the Nigerian Communications (Enforcement Process, etc.) Regulation 2005, and the Guidelines for the Provision of Internet Service.
- **National Identity Management Commission (NIMC):** NIMC is the data protection authority under the NIMC Act 2007 and the Mandatory Use of the NIN Regulations 2015 and 2017.
- **Central Bank of Nigeria (CBN):** CBN is the data protection authority under the Consumer Protection Framework 2016 and the Credit Reporting Act 2017.
- **The Federal Ministry of Health:** The health ministry is the data protection authority under the National Health Act.

2 Definitions

2.1 Please provide the key definitions used in the relevant legislation:

- **“Consent”** (of the Data Subject): “any freely given, specific, informed and unambiguous indication of the Data Subject’s wishes by which he or she, through a statement or a clear affirmative action, signifies agreement to the processing of Personal Data relating to him or her”.
- **“Data Administrator”**: “a person or an organization that processes data”.
- **“Data Controller”**: “a person who either alone, jointly with other persons or in common with other persons or a statutory body determines the purposes for and the manner in which Personal Data is processed or is to be processed”.
- **“Data Subject”**: “any person, who can be identified, directly or indirectly, by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity”.
- **“Personal Data”**: “any information relating to an identified or identifiable natural person (‘Data Subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. It can be anything from a name, address, a photo, an email address, bank details, posts on social networking websites, medical information, and other unique identifier such as but not limited to MAC address, IP address, IMEI number, IMSI number, SIM, Personal Identifiable Information (PII) and others”.
- **“Personal Data Breach”**: “a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed”.
- **“Personal Identifiable Information (PII)”**: “information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in a context”.
- **“Processing”**: “any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction”.
- **“Sensitive Personal Data”**: “data relating to religious or other beliefs, sexual orientation, health, race, ethnicity, political views, trades union membership, criminal records or any other sensitive personal information”.
- **“Third Party”**: “any natural or legal person, public authority, establishment or any other body other than the Data Subject, the Data Controller, the Data Administrator and the persons who are engaged by the Data Controller or the Data Administrator to process Personal Data”.

3 Territorial Scope

3.1 Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to those laws?

Only the Regulation applies to businesses established in other jurisdictions. According to the Regulation, it applies to:

(a) all transactions for the processing of personal data, regardless of the means by which the data processing is being conducted or intended to be conducted in respect of natural persons in Nigeria; and

(b) all natural persons residing in Nigeria or residing outside Nigeria who are citizens of Nigeria.

4 Key Principles

4.1 What are the key principles that apply to the processing of personal data?

- **Transparency**
  When collecting data, the specific purpose of collection must be made known to the data subject before obtaining consent.

- **Lawful basis for processing**
  Processing shall be lawful if at least one of the following applies:
  a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;  
  b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject before entering into a contract;  
  c) processing is necessary for compliance with a legal obligation to which the controller is subject;  
  d) processing is necessary in order to protect the vital interests of the data subject or of another natural person; and  
  e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of an official public mandate vested in the controller.
5 Individual Rights

5.1 What are the key rights that individuals have in relation to the processing of their personal data?

Before a data controller may collect the personal data of a data subject, the Regulation requires that the controller informs the data subject of the following rights:

- **Right of access to data or copies of data**
  A data subject has the right to access personal data provided to the controller.

- **Right to rectification of errors**
  A data subject has the right to rectify his or her personal data. This ensures data accuracy.

- **Right to deletion/right to be forgotten**
  A data subject has the right to have his or her personal data deleted, erased, or forgotten by the controller, subject to the conditions stated in the Regulation.

- **Right to object to processing**
  A data subject has the right to object to processing. For this purpose, a data subject shall have the option to be expressly and manifestly offered the mechanism for objection to any form of data processing free of charge.

- **Right to restrict processing**
  A data subject has the right to restrict processing of his or her personal data. Once processing has been restricted, such personal data shall, except for storage, only be processed with the data subject’s consent or for the establishment, exercise, or defence of legal claims or for the protection of the rights of another natural or legal person, or for public interest.

- **Right to data portability**
  A data subject has the right to data portability. In exercising his or her right to data portability, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.

- **Right to withdraw consent**
  A data subject has the right to be informed by the controller of his or her right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal.

- **Right to object to marketing**
  A data subject has the right to object to the processing of his or her data for marketing. The data subject’s personal data shall be safeguarded at all times.

- **Other key rights – please specify**
  - This is not applicable.

- **Right to structured data**
  - A data subject has the right to receive the personal data which he or she has provided to a controller, in a commonly used structured and machine-readable format.

- **Right to make requests to the data controller without charge**
  - A data controller’s responses to requests are free of charge as long as the data subject’s requests are not manifestly unfounded or excessive.

- **Right to make complaint to the Data Protection Authority**
  - This right is to enable a data subject to seek remedy in respect of any alleged breach of his or her data privacy rights whenever an issue arises.

6 Registration Formalities and Prior Approval

6.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?

The Regulation requires that a data controller who processes the personal data of more than 1,000 data subjects in a period of six months must submit a soft copy of the summary of the audit to NITDA. On an annual basis, a data controller who processes the personal data of more than 2,000 data subjects in a period of 12 months shall, not later than 15 March of the following year, submit a summary of its data protection audit to NITDA. NITDA is also empowered to register and license Data Protection Compliance Organisations who shall, on behalf of the Agency, monitor, audit, conduct training, and provide data protection compliance consulting to all data controllers under this Regulation.

6.2 If such registration/notification is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?

The Regulation requires that within six months after the Regulation is issued, each organisation shall conduct a detailed audit of its privacy and data protection practices. The following information must be stated in the audit:

- personally identifiable information the organisation collects on employees of the organisation and members of the public;
any purpose for which the personally identifiable information is collected;
any notice given to individuals regarding the collection and use of personal information relating to that individual;
any access given to individuals to review, amend, correct, supplement, or delete personal information relating to that individual;
whether or not consent is obtained from an individual before personally identifiable information is collected, used, transferred, or disclosed and any method used to obtain consent;
the policies and practices of the organisation for the security of personally identifiable information;
the policies and practices of the organisation for the proper use of personally identifiable information;
organisation policies and procedures for privacy and data protection;
the policies and procedures of the organisation for monitoring and reporting violations of privacy and data protection policies; and
the policies and procedures of the organisation for assessing the impact of technologies on the stated privacy and security policies.

6.3 On what basis are registrations/notifications made (e.g., per legal entity, per processing purpose, per data category, per system or database)?

The basis for registration/notification is per database, specifically where a data controller processes personal data of more than 1,000 data subjects in a period of six months or where a data controller processes personal data of more than 2,000 data subjects in a year.

6.4 Who must register with/notify the data protection authority (e.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation)?

Data controllers are required to have Data Protection Officers who will ensure that the data controller adheres to the Regulation, relevant data privacy instruments, and data protection directives of the data controller.

6.5 What information must be included in the registration/notification (e.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes)?

Please see answer in 6.2 above.

6.6 What are the sanctions for failure to register/notify where required?

There are no specific sanctions for failing to register/notify NITDA of processing activities. However, by virtue of section 17(4) of the NITDA Act 2007 (the principal Act), a person or body corporate that fails to comply with the guidelines and standards prescribed by NITDA commits an offence. For a first offence, the penalty is a fine of N200,000 (approx. €500) or imprisonment for a term of one year, or both fine and imprisonment. For a second and subsequent offence, the penalty is a fine of N500,000 (approx. €1,240) or imprisonment for a term of three years, or both.

6.7 What is the fee per registration/notification (if applicable)?

No prescribed fee for registration has been specified in the Regulation or made by NITDA.

6.8 How frequently must registrations/notifications be renewed (if applicable)?

Registration/notification is to be made annually.

6.9 Is any prior approval required from the data protection regulator?

Apart from the approval of Data Protection Compliance Organisations (DPCOs) through registration and licensing by NITDA, there is no provision for prior approval from NITDA.

6.10 Can the registration/notification be completed online?

This does not apply in our jurisdiction.

6.11 Is there a publicly available list of completed registrations/notifications?

This does not apply in our jurisdiction.

6.12 How long does a typical registration/notification process take?

This does not apply in our jurisdiction.

7 Appointment of a Data Protection Officer

7.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.

The appointment of a Data Protection Officer is mandatory.

7.2 What are the sanctions for failing to appoint a Data Protection Officer where required?

The same penalty stated in question 6.6 above applies.

7.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect of his or her role as a Data Protection Officer?

This does not apply in our jurisdiction.

7.4 Can a business appoint a single Data Protection Officer to cover multiple entities?

The Regulation does not specify whether a single Data Protection Officer can cover multiple entities.
7.5 Please describe any specific qualifications for the Data Protection Officer required by law.

There are no specific qualifications for a Data Protection Officer. What the Regulation requires is that a Data Protection Officer may be outsourced and shall be a “verifiably competent firm or person”.

7.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?

The Data Protection Officer’s responsibilities as required by law and best practice include the following:

- Ensure that the data controller or processor adheres to the Regulation and relevant data privacy instruments and data protection directives of the data controller.
- Ensure that the data controller or processor has a continuous capacity-building mechanism for his or her own benefit and the generality of the personnel involved in any form of data processing.
- Liaise with regulators in respect of data protection.
- Work with Data Protection Compliance Organisations whose duty it is to provide monitoring, auditing, training, and data protection compliance consulting to data controllers under the Regulation.
- Ensure that the data controller complies with the requirement of periodical data audits, to be submitted to NITDA.
- Ensure that the data controller has policies and procedures for privacy and data protection, including having a publicly available privacy policy.

7.7 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?

There is no requirement that the appointment of a Data Protection Officer be registered with NITDA or any other relevant authority.

7.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?

There is no express provision for the Data Protection Officer to be named in a public-facing privacy notice. However, the Regulation requires that before collecting personal data from a data subject, the controller must provide the data subject with contact details of the Data Protection Officer.

8 Appointment of Processors

8.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?

Yes. A business that appoints a processor to process personal data on its behalf must have a contract with the processor.

8.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?

The Regulation requires that the agreement must be in writing and any person engaging a third party to process the data obtained from data subjects shall ensure adherence to the Regulation.

9 Marketing

9.1 Please describe any legislative restrictions on the sending of electronic direct marketing (e.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?).

The Regulation does not restrict electronic marketing, but the NCC Consumer Code of Practice Regulation restricts telemarketing communications. The restriction applies to telecommunication companies. Before a telecommunications company is able to telemarket, it must disclose to the subscriber: (a) the third party on whose behalf the telemarketing communication is made; (b) the purpose of the communication; (c) the full price of the product or service which is being telemarket; and (d) confirmation that the individual has an absolute right to cancel the agreement for purchase, lease, or other supply of any product or service within seven days of the telemarketing communication via a stated toll-free telephone number. Also, to control telecommunication marketing by enabling subscribers have an opt-out option, NCC introduced a DO-NOT-DISTURB code (2442) in 2016. Once activated, it does not allow a subscriber to receive unsolicited messages from the operators.

9.2 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.).

No. The restrictions do not apply to marketing sent from other jurisdictions, but if the marketing is sent through a local agent or organisation, they may.

9.3 Do the restrictions noted above apply to marketing sent from other jurisdictions?

Of the data protection authorities under the relevant legislation and regulations, NCC has been the most active in enforcing breaches of marketing restrictions.
9.5 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?

The Regulation is silent about the purchase of marketing lists from third parties, but under the Regulation, any collection or sharing of personal data is subject to the lawful consent of the data subject. Therefore, this requirement to obtain the data subject’s consent applies. Also, under the Consumer Code of Practice Regulations and the Registration of Telephone Subscribers Regulation, it is illegal for telecommunication service providers to provide third parties with access to a subscriber’s personal data.

9.6 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?

There are no penalties stipulated under the Regulation, but under the Nigerian Communications (Enforcement Processes, etc.) Regulations of 2005, telecommunication services providers who breach marketing restrictions face a fine of N10,000,000 (approx. €24,380).

10 Cookies

10.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).

The Regulation requires that any medium through which personal data is collected or processed shall display a simple and conspicuous privacy policy which shall, amongst other things, contain technical methods used to collect and store personal information, including cookies, JWT web tokens, etc.

10.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?

This does not apply in our jurisdiction.

10.3 To date, has/have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?

This does not apply in our jurisdiction.

10.4 What are the maximum penalties for breaches of applicable cookie restrictions?

This does not apply in our jurisdiction.

11 Restrictions on International Data Transfers

11.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.

Any transfer of personal data to a foreign country or to an international organisation is subject to the provisions of the Regulation and the supervision of the Attorney General of the Federation. Mainly, it is required that the foreign country has adequate protection for the international transfer of personal data.

11.2 Please describe the mechanisms businesses typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).

Businesses avoid restrictions on the international transfer of personal data by taking advantage of certain exceptions. These include: (a) obtaining the data subject’s explicit and informed consent to the proposed transfer and informing the data subject of possible risks; (b) ensuring that the transfer is necessary for the performance of a contract between the data subject and the controller or to implement precontractual measures; and (c) ensuring that the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person.

11.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.

Yes. The transfer of personal data to other jurisdictions requires the approval of NITDA with the Attorney General of the Federation. This is regardless of the type of transfer. The Attorney General will consider whether the foreign country or international organisation: (a) has adequate protection for data and privacy; (b) has rules and security measures for the transfer of personal data to another foreign country; (c) has effective implementation mechanisms; (d) has independent supervisory authorities to which an international organisation is subject; and (e) is internationally committed, in relation to personal data protection, to legally binding instruments, including multilateral and regional participation.

12 Whistle-blower Hotlines

12.1 What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?

This does not apply in our jurisdiction.

12.2 Is anonymous reporting prohibited, strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do businesses typically address this issue?

This does not apply in our jurisdiction.
13 CCTV

13.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?

Though the Regulation does not contain provisions for the use of CCTV, it falls under the scope of the Regulation by virtue of section 1.2 of the Regulation. This is because it applies “to all transactions intended for the processing of personal data and to actual processing of personal data notwithstanding the means by which the data processing is being conducted or intended to be conducted and in respect of natural persons in Nigeria”.

13.2 Are there limits on the purposes for which CCTV data may be used?

This does not apply in our jurisdiction.

14 Employee Monitoring

14.1 What types of employee monitoring are permitted (if any), and in what circumstances?

None of the data protection legislation provides for employee monitoring, but employees in Nigeria or of Nigerian descent are data subjects under the Regulation; thus data processing principles and data subject rights apply.

14.2 Is consent or notice required? Describe how employers typically obtain consent or provide notice.

The general provision on obtaining the data subject’s lawful consent under the Regulation applies.

14.3 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?

This does not apply in our jurisdiction.

15 Data Security and Data Breach

15.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?

Yes. There is a general obligation to ensure the security of personal data. The Regulation requires that anyone involved in data processing or the control of data must have security measures to protect such data.

Both data controllers and processors are responsible for ensuring that security measures are put in place to safeguard personal data. These security measures include protecting systems from hackers, setting up firewalls, storing data securely and ensuring authorised access only, encrypting data, developing organisational policy for handling personal data (and other sensitive or confidential data), ensuring emailing systems’ protection, and continuous capacity-building for staff.

15.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

No. There is no legal requirement to report data breaches to data protection authorities.

15.3 Is there a legal requirement to report data breaches to affected data subjects? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

No. There is no legal requirement to report data breaches to data subjects.

15.4 What are the maximum penalties for data security breaches?

In addition to any other criminal liability, the following penalties apply to data breaches under the Regulation:

(a) in the case of a data controller dealing with more than 10,000 data subjects, payment of the fine of 2% of Annual Gross Revenue of the preceding year or payment of the sum of N10 million (approx. €24,800), whichever is greater; and

(b) in the case of a data controller dealing with less than 10,000 data subjects, payment of the fine of 1% of the Annual Gross Revenue of the preceding year or payment of the sum of N2 million (approx. €4,900), whichever is greater.
# Enforcement and Sanctions

## 16.1 Describe the enforcement powers of the data protection authority(ies).

<table>
<thead>
<tr>
<th>Investigatory Power</th>
<th>Civil/Administrative Sanction</th>
<th>Criminal Sanction</th>
</tr>
</thead>
<tbody>
<tr>
<td>NITDA is entitled to receive submissions of copies of the summary of conducted audits from data controllers, which aids its investigatory powers for the purpose of identifying real or potential data breaches under the Regulation.</td>
<td>Not applicable.</td>
<td>By virtue of section 17(4) of the NITDA Act 2007, the penalty for breach of the provisions of the Regulations is a fine of N200,000 (approx. €500) or imprisonment for a term of one year for a first offence. For a second or subsequent offence, the civil/administrative sanction is a fine of N500,000 (approx. €1,240) or imprisonment for a term of three years.</td>
</tr>
<tr>
<td>NITDA registers and licenses Data Protection Compliance Organisations who audit and monitor the data protection policies of data controllers and also train data controllers on data protection on NITDA’s behalf.</td>
<td>Imposes civil/administrative sanctions such as refunds, suspension from inter-bank activities, denial of approvals, publication of infractions and sanctions, monetary penalties, product recall, suspension/removal of Board/management staff/employees, referral to law enforcement agencies for prosecution, revocation of banking licence, etc.</td>
<td>Under section 20(1)(c) of the Credit Reporting Act, any person who intentionally or negligently discloses credit information in contravention of the provisions of the Act commits an offence punishable under section 23 of the Act. Upon conviction, a minimum fine of N10 million (approx. €23,000) or a 10-year imprisonment applies, or both. The same punishment applies to any person who intentionally or wilfully obtains information from a credit bureau under false pretence or for a purpose other than a permissible purpose.</td>
</tr>
<tr>
<td>NITDA is charged with the duty of setting up the Administrative Redress Panel, whose duty it is to carry out the following functions: (1) investigating allegations of any breach of the provisions of this Regulation; (2) inviting any party to respond to allegations made against it within seven days; (3) issuing administrative orders to protect the subject matter of the allegation pending the outcome of investigation; (4) concluding the investigation and determining the appropriate redress within 28 working days.</td>
<td>Imposes civil/administrative sanctions such as refunds, suspension from inter-bank activities, denial of approvals, publication of infractions and sanctions, monetary penalties, product recall, suspension/removal of Board/management staff/employees, referral to law enforcement agencies for prosecution, revocation of banking licence, etc.</td>
<td>Under section 20(1)(c) of the Credit Reporting Act, any person who intentionally or negligently discloses credit information in contravention of the provisions of the Act commits an offence punishable under section 23 of the Act. Upon conviction, a minimum fine of N10 million (approx. €23,000) or a 10-year imprisonment applies, or both. The same punishment applies to any person who intentionally or wilfully obtains information from a credit bureau under false pretence or for a purpose other than a permissible purpose.</td>
</tr>
<tr>
<td>CBN conducts investigations when necessary, and its findings form the basis for management decisions.</td>
<td>CBN reviews, monitors and supervises the operations of credit bureaux under the Credit Reporting Act, and imposes pecuniary and other penalties for the contravention of the Credit Reporting Act.</td>
<td>Under section 20(1)(c) of the Credit Reporting Act, any person who intentionally or negligently discloses credit information in contravention of the provisions of the Act commits an offence punishable under section 23 of the Act. Upon conviction, a minimum fine of N10 million (approx. €23,000) or a 10-year imprisonment applies, or both. The same punishment applies to any person who intentionally or wilfully obtains information from a credit bureau under false pretence or for a purpose other than a permissible purpose.</td>
</tr>
<tr>
<td>CBN monitors compliance and imposes penalties in the event of any breaches. It administers the Registration of Telephone Subscribers Regulation 2011 (RTS Regulations). Section 21 penalises entities that retain, duplicate, or deal with subscribers’ information in a manner which contravenes the Regulations.</td>
<td>CBN administers the Consumer Code of Practice Regulations and oversees compliance by licensees. Section 55 of the Regulations gives NCC the authority to investigate complaints in the event of any breach of the Code.</td>
<td>Under section 20(1)(c) of the Credit Reporting Act, any person who intentionally or negligently discloses credit information in contravention of the provisions of the Act commits an offence punishable under section 23 of the Act. Upon conviction, a minimum fine of N10 million (approx. €23,000) or a 10-year imprisonment applies, or both. The same punishment applies to any person who intentionally or wilfully obtains information from a credit bureau under false pretence or for a purpose other than a permissible purpose.</td>
</tr>
<tr>
<td>NCC administers the Consumer Code of Practice Regulations and oversees compliance by licensees. Section 55 of the Regulations gives NCC the authority to investigate complaints in the event of any breach of the Code.</td>
<td>Not applicable.</td>
<td>For any violation of the Regulations, the fine is N5 million (approx. €12,350) and a further N500,000 (approx. €1,350) per day for as long as the contravention persists after NCC’s notice expires.</td>
</tr>
<tr>
<td>NCC monitors compliance and imposes penalties in the event of any breaches. It administers the Registration of Telephone Subscribers Regulation 2011 (RTS Regulations). Section 21 penalises entities that retain, duplicate, or deal with subscribers’ information in a manner which contravenes the Regulations.</td>
<td>NCC administers the Consumer Code of Practice Regulations and the RTS Registration by virtue of the Nigerian Communications (Enforcement Process, etc.) Regulation 2005.</td>
<td>For violating section 21 of the RTS Regulations, the sanction is N200,000 (approx. €500) per subscription medium. If the entity uses subscribers’ information in any business, commercial, or other transactions inconsistent with the Regulations, the entity is liable to a penalty of N1 million (approx. €2,500) per subscription medium.</td>
</tr>
<tr>
<td>NCC enforces the Consumer Code of Practice Regulations and the RTS Registration by virtue of the Nigerian Communications (Enforcement Process, etc.) Regulation 2005.</td>
<td>Not applicable.</td>
<td>NIMC, as the data protection authority in the national identity management sector, ensures the protection and security (including cybersecurity) of any data collected, stored, or maintained in respect of the National Identity Database. Under section 28(1) of the NIMC Act, it is an offence for a person to: access data or information contained in the database; refuse to provide relevant data or information to the Commission; or knowingly or recklessly provide false information to the Commission.</td>
</tr>
</tbody>
</table>
## Investigatory Power

<table>
<thead>
<tr>
<th>Relevant Law Enforcement Agencies</th>
<th>Civil/Administrative Sanction</th>
<th>Criminal Sanction</th>
</tr>
</thead>
<tbody>
<tr>
<td>♦ Under the Cybercrimes Act, a law enforcement agency may request a service provider to keep any traffic data, subscriber information, and content or non-content information or release any information it has stored. This must be for law-enforcement purposes only.</td>
<td>♦ Not applicable.</td>
<td>♦ It is an offence for a service provider to fail to keep any traffic data, subscriber information, and content or non-content information, or to refuse to release to law enforcement agencies or by order of court any information it has stored. Upon conviction, the punishment is imprisonment for a term of not more than three years or a fine of not more than NGN 7 million (approx. €17,300), or both fine and imprisonment.</td>
</tr>
<tr>
<td>♦ For the purpose of criminal investigations or proceedings, law-enforcement agencies are permitted to intercept electronic communication, subject to obtaining a court order.</td>
<td></td>
<td>♦ It is an offence for a service provider to refuse to assist a law enforcement agency to intercept electronic communication. Upon conviction, the service provider is liable to a fine of not less than N10 million (approx. €23,000). Each director, manager, or officer of the service provider will also be liable on conviction to not more than three years’ imprisonment or a N7 million fine (approx. €17,300), or to both fine and imprisonment.</td>
</tr>
</tbody>
</table>

## 16.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?

To the extent that a data protection authority’s decision to ban a particular processing activity is within its powers under the relevant legislation, a data protection authority may issue a ban. Therefore, recourse to a court is not required.

## 16.3 Describe the data protection authority’s approach to exercising those powers, with examples of recent cases.

The data protection authorities tend to give businesses adequate time before taking any enforcement actions. For instance, NCC recently handed down a $5.2 billion fine against MTN after MTN failed to disconnect Subscribers Identification Modules (SIM) with improper registration. MTN had up to 5.2 million unregistered customer lines. MTN was fined $1,000 for each unregistered SIM, amounting to $5.2 billion.

## 16.4 Does the data protection authority ever exercise its powers against businesses established in other jurisdictions? If so, how is this enforced?

A data protection authority may exercise its powers against businesses established in other jurisdictions, as long as those businesses control or process the data of natural persons in Nigeria or residing outside Nigeria who are citizens of Nigeria.

For enforcement, NITDA and the relevant authorities (who are data protection authorities under the relevant legislation) are required to take appropriate steps to develop international cooperation mechanisms to facilitate the effective enforcement of legislation for the protection of personal data through notification, complaint referral, investigative assistance, and information exchange; international mutual assistance is expected in the enforcement of data protection legislation internationally.

## 17 E-discovery / Disclosure to Foreign Law Enforcement Agencies

### 17.1 How do businesses typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?

There is no standard response for responding to foreign e-discovery requests.

### 17.2 What guidance has/have the data protection authority(ies) issued?

No guidance has been issued in our jurisdiction.

## 18 Trends and Developments

### 18.1 What enforcement trends have emerged during the previous 12 months? Describe any relevant case law.

The Regulation, issued by NITDA on 25 January 2019, is relatively new. Enforcement trends are yet to emerge. But NCC’s $5.2 billion fine against MTN in October 2015 by virtue of NCC’s powers under section 20(1) of the Registration of Telephone Subscribers Regulations (TSR) 2011 is one decision that data controllers and processors cannot afford to ignore.

### 18.2 What “hot topics” are currently a focus for the data protection regulator?

Before the new Regulation was made, there were concerns from various quarters about the enforceability of the provisions of NITDA’s Data Protection Guidelines 2013, which have been effectively repealed. With the scope of the new Regulation applying to personal data of natural persons in Nigeria and Nigerians outside the country, the “hot topic” is whether relevant data protection authorities in Nigeria have the powers and the enforcement mechanisms to ensure compliance by international organisations. Whether this regulation will also spur data protection authorities to step up their game against local data controllers or processors who violate the privacy of data subjects in various industries and sectors, remains to be seen.
Senator Iyere Ihenyen specialises in information technology and intellectual property law. He is a thought leader in both areas.

A DataGuidance by OneTrust expert on data protection and privacy for Nigeria, Senator advises local and foreign clients on data protection and privacy.

Tech-savvy, Senator works with innovators in the technology space, from intellectual-property-driven innovations to disruptive decentralised ledger technology-powered innovations. He advises and consults for a number of players in the technology space, including Kurecoin and Kurepay, Paxful, and SUREBANQA. Following his work in the space, Senator is Vice Chairman (Policy & Regulations) of the Stakeholders in Blockchain Technology Association of Nigeria (SiBAN) and a Trustee of the African ICT Foundation.

He is a member of the Information & Communications Technology; Intellectual Property; and Sports, Entertainment & Media Committees of the Nigerian Bar Association’s Section on Business Law.

Senator is the Lead Partner at Infusion Lawyers. He heads the Intellectual Property & Information Technology team.

Rita Anwiri Chindah, ACIArb specialises in intellectual property, information technology, and Arbitration and Alternative Dispute Resolution (ADR).

A Master’s degree holder in Intellectual Property & Information Technology from the University of Derby, UK, Rita is knowledgeable in data protection and privacy, media law, copyright, industrial designs, trademarks, and patents.

Rita has some experience advising startups and companies on intellectual property and technology in the digital age. She also brings her knowledge in Arbitration and ADR to bear, helping clients proactively minimise risks.

Rita is a member of: the Nigerian Bar Association (NBA) Section on Business Law, within the Committees on Arbitration and Alternative Dispute Resolution and Information and Communications Technology; the Chartered Institute of Arbitrators (UK), Nigeria Branch; and the Nigerian Institute of Management.

Rita heads the IP & IT Advocacy team at Infusion Lawyers.
Norway

1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

The principal data protection legislation in the EU is Regulation (EU) 2017/679 (the “General Data Protection Regulation” or “GDPR”). The GDPR repeals Directive 95/46/EC (the “Data Protection Directive”) and has thereby led to increased (though not total) harmonisation of data protection law across the EU Member States. As Norway is not an EU Member State but part of European Economic Area (“EEA”), the GDPR had to be incorporated into the EEA Agreement before it could be implemented into national law. The GDPR was incorporated into national law by means of the new Personal Data Act, which has been in effect since 20 July 2018.

1.2 Is there any other general legislation that impacts data protection?


In addition, the Marketing Control Act (Act of 9 January 2009 No. 2) regulates marketing communications (see question 9.1).

1.3 Is there any sector-specific legislation that impacts data protection?

Various pieces of sectorial legislation impact data protection, including the Personal Health Data Filing System Act (Act of 20 June 2014 No. 43) and the various regulations pertaining thereto. Furthermore, the Act on Patient Medical Records (Act of 20 June 2014 No. 42), the Health Research Act (Act of 20 June 2008 No. 44), the Therapeutic Biobanks Act (Act of 21 February 2003 No. 12), chapter 8 of the Health Personnel Act (Act of 2 July 1999 No. 64), chapter 5 of the Patient Rights Act (Act of 2 July 1999 No. 63), the Act on Police Records (Act of 28 May 2010 No. 16), the Schengen Information Systems Act (Act of 16 July 1999 No. 66) and its regulations, and the Currency Exchange Register Act (Act of 28 May No. 29) also impact data protection.

These sector-specific laws were retained after the implementation of the GDPR but relevant provisions were amended to ensure compliance and coherence with the GDPR and the new Personal Data Act.

1.4 What authority(ies) are responsible for data protection?

The Norwegian Data Protection Authority (hereinafter referred to as “NDPA”) oversees and enforces the Personal Data Act and the GDPR. It is an independent administrative body that reports annually to the Storting (Parliament). The current Data Protection Commissioner (direktør) is Bjørn Erik Thon, who was appointed in August 2010 and whose appointment was renewed for another six-year term from August 2016.

Data controllers within the health sector are additionally regulated by the various pieces of health sector legislation relating to the processing of medical health data.

The Norwegian Communications Authority oversees and enforces the Electronic Communications Act, including compliance with the cookie provisions.

2 Definitions

2.1 Please provide the key definitions used in the relevant legislation:

- **“Personal Data”**
  “Personal Data” means any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

- **“Processing”**
  “Processing” means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

- **“Controller”**
  “Controller” means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
What are the key principles that apply to the processing of personal data?

Transparency
Personal data must be processed lawfully, fairly and in a transparent manner. Controllers must provide certain minimum information to data subjects regarding the collection and further processing of their personal data. Such information must be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

Lawful basis for processing
Processing of personal data is lawful only if, and to the extent that, it is permitted under EU data protection law. The GDPR provides an exhaustive list of legal bases on which personal data may be processed, of which the following are the most relevant for businesses: (i) prior, freely given, specific, informed and unambiguous consent of the data subject; (ii) contractual necessity (i.e., the processing is necessary for the performance of a contract to which the data subject is a party, or for the purposes of pre-contractual measures taken at the data subject’s request); (iii) compliance with legal obligations (i.e., the controller has a legal obligation, under the laws of the EU or an EU Member State, to perform the relevant processing); or (iv) legitimate interests (i.e., the processing is necessary for the purposes of legitimate interests pursued by the controller, except where the controller’s interests are overridden by the interests, fundamental rights or freedoms of the affected data subjects).

Please note that businesses require stronger grounds to process sensitive personal data. The processing of sensitive personal data is only permitted under certain conditions, of which the most relevant for businesses are: (i) explicit consent of the affected data subject; (ii) the processing is necessary in the context of employment law; or (iii) the processing is necessary for the establishment, exercise or defence of legal claims.

Purpose limitation
Personal data may only be collected for specified, explicit and legitimate purposes and must not be further processed in a manner that is incompatible with those purposes. If a controller wishes to use the relevant personal data in a manner that is incompatible with the purposes for which they were initially collected, it must be able to rely on the data subject’s consent as a legal basis or the further processing must be permitted by law.

Data minimisation
Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which those data are processed. A business should only process the personal data that it actually needs to process in order to achieve its processing purposes.

Proportionality
The cumulative requirements of the principle of proportionality are fulfilled by compliance with the requirements of other basic principles.

Retention
Personal data must be kept in a form that permits the identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) of the
GDPR, subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of the data subject.

**Other key principles – please specify**

- **Accuracy**
  Personal data must be accurate and, where necessary, kept up to date. A business must take every reasonable step to ensure that personal data that are inaccurate are either erased or rectified without delay.

- **Data security**
  Personal data must be processed in a manner that ensures appropriate security of those data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

- **Accountability**
  The controller is responsible for, and must be able to demonstrate, compliance with the data protection principles set out above.

**5 Individual Rights**

**5.1 What are the key rights that individuals have in relation to the processing of their personal data?**

- **Right of access to data/copies of data**
  A data subject has the right to obtain from a controller the following information in respect of the data subject’s personal data: (i) confirmation of whether, and where, the controller is processing the data subject’s personal data; (ii) information about the purposes of the processing; (iii) information about the categories of data being processed; (iv) information about the categories of recipients with whom the data may be shared; (v) information about the period for which the data will be stored (or the criteria used to determine that period); (vi) information about the existence of the rights to erasure, to rectification, to restriction of processing and to object to processing; (vii) information about the existence of the right to complain to the relevant data protection authority; (viii) where the data were not collected from the data subject, information as to the source of the data; and (ix) information about the existence of, and an explanation of the logic involved in, any automated processing that has a significant effect on the data subject. Additionally, the data subject may request a copy of the personal data being processed.

- **Right to rectification of errors**
  Controllers must ensure that inaccurate or incomplete data are erased or rectified. Data subjects have the right to rectification of inaccurate personal data.

- **Right to deletion/right to be forgotten**
  Data subjects have the right to erasure of their personal data (the “right to be forgotten”) if: (i) the data are no longer needed for their original purpose (and no other lawful purpose exists); (ii) the lawful basis for the processing is the data subject’s consent, the data subject withdraws that consent, and no other lawful ground exists; (iii) the data subject exercises the right to object, and the controller has no overriding grounds for continuing the processing; (iv) the data have been processed unlawfully; or (v) erasure is necessary for compliance with EU law or national data protection law.

- **Right to object to processing**
  Data subjects have the right to object, on grounds relating to their particular situation, to the processing of personal data where the basis for that processing is either the performance of a task carried out in the public interest or in the exercise of official authority, or where the basis for the processing is the legitimate interest of the controller. The controller must cease such processing unless it demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the relevant data subject or requires the data in order to establish, exercise or defend legal rights.
  The data subject also has a right to object to processing for direct marketing purposes; see below.

- **Right to restrict processing**
  Data subjects have the right to restrict the processing of personal data, which means that the data may only be held by the controller, and may only be used for limited purposes if: (i) the accuracy of the data is contested by the data subject (and only for as long as it takes to verify that accuracy); (ii) the processing is unlawful and the data subject requests restriction (as opposed to exercising the right to erasure); (iii) the controller no longer needs the data for their original purpose, but the data are still required by the data subject to establish, exercise or defend legal claims; or (iv) verification of overriding grounds is pending, in the context of the data subject’s exercise of his/her right to object to processing.

- **Right to data portability**
  Data subjects have a right to receive a copy of their personal data in a commonly used machine-readable format, and to transmit their personal data from one controller to another or have the data transmitted directly between controllers. This right applies where the basis for the processing is the data subject’s consent or where the processing is necessary for the performance of a contract with the data subject.

- **Right to withdraw consent**
  A data subject has the right to withdraw his/her consent at any time. The withdrawal of consent does not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject must be informed of the right to withdraw consent. It must be as easy to withdraw consent as to give it.

- **Right to object to marketing**
  Data subjects have the right to object to the processing of personal data for the purpose of direct marketing, including profiling.

- **Right to complain to the relevant data protection authority(ies)**
  Data subjects have the right to lodge complaints concerning the processing of their personal data with the NDPA, if the data subjects live or work in Norway or the alleged infringement occurred in Norway.

**Other key rights – please specify**

- **Right to basic information**
  Data subjects have the right to be provided with information on the identity of the controller, the reasons for processing their personal data and other relevant information necessary to ensure the fair and transparent processing of personal data.

- **Automated individual decision-making**
  The data subject has the right not to be subject to a fully automated decision, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her, except if the decision: (i) is necessary for the entering into, or performance of, a contract with the data subject; (ii) is authorised by EU or national law to which the controller is subject and which lays down suitable measures to safeguard the data subject’s rights and freedoms and legitimate interest; or (iii) is based on the data subject’s explicit consent. Where the decision is carried out on the grounds specified in (i) or (ii) as aforementioned, the data subject has the right to
obtain human intervention by the controller, to express his or her view and to contest the decision. Automated decisions may not be based on sensitive personal data unless the processing is based on either the data subject’s consent or is for reasons of substantial public interest based on EU or national law and suitable measures to safeguard the data subject’s rights and freedoms and legitimate interests are in place.

6 Registration Formalities and Prior Approval

6.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?

There is no legal obligation on businesses to register with or notify the NDPA in respect of their processing activities. Note, however, that there are some transitional provisions related to prior approval/licences given prior to the implementation of the GDPR in Norway; most notably licences to perform credit reporting, licences to carry out integrity due diligence, and licences to perform doping controls at certain fitness establishments.

Please also note that, in some instances, businesses are obliged to consult with the NDPA before the processing starts. This especially pertains to certain high-risk processing. The government has the power to implement specific regulations regarding prior consultation and prior authorisation, but so far, no such regulations have been enacted.

6.2 If such registration/notification is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?

This is not applicable.

6.3 On what basis are registrations/notifications made (e.g., per legal entity, per processing purpose, per data category, per system or database)?

This is not applicable.

6.4 Who must register with/notify the data protection authority (e.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation)?

This is not applicable.

6.5 What information must be included in the registration/notification (e.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes)?

This is not applicable.

6.6 What are the sanctions for failure to register/notify where required?

This is not applicable.

6.7 What is the fee per registration/notification (if applicable)?

This is not applicable.

6.8 How frequently must registrations/notifications be renewed (if applicable)?

This is not applicable.

6.9 Is any prior approval required from the data protection regulator?

No prior approval from the data protection regulator is required. However, according to the new Personal Data Act, the NDPA may permit the processing of special categories of personal data where the processing is necessary for important public interests. In such cases, the NDPA shall lay down conditions to protect the data subject’s fundamental rights and interests. The government has the power to adopt regulations to allow the processing of special categories of personal data where this is necessary for important public interests. Such regulations shall lay down appropriate and special measures to protect the data subject’s fundamental rights and interests.

6.10 Can the registration/notification be completed online?

This is not applicable.

6.11 Is there a publicly available list of completed registrations/notifications?

This is not applicable.

6.12 How long does a typical registration/notification process take?

This is not applicable.

7 Appointment of a Data Protection Officer

7.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.

The appointment of a Data Protection Officer for controllers or processors is mandatory in some circumstances, including where the core activity of the data controller consists of: (i) large-scale regular and systematic monitoring of individuals; or (ii) large-scale processing of special categories of personal data. The appointment of a Data Protection Officer is also mandatory where processing is carried out by a public authority or body. In the preparatory works to the Personal Data Act, the Justice Department specifies that this comprises the administrative bodies that fall within section 2, first
paragraph, letter a of the Public Administration Act, i.e., any state, county authority or municipal body.

Where a business designates a Data Protection Officer voluntarily, the requirements of the GDPR apply as though the appointment was mandatory.

7.2 What are the sanctions for failing to appoint a Data Protection Officer where required?

In the circumstances where the appointment of a Data Protection Officer is mandatory, failure to comply may result in the wide range of penalties available under the GDPR.

7.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect of his or her role as a Data Protection Officer?

The appointed Data Protection Officer should not be dismissed or penalised for performing their tasks and should report directly to the highest management level of the controller or processor.

7.4 Can a business appoint a single Data Protection Officer to cover multiple entities?

A single Data Protection Officer is permitted by a group of undertakings provided that the Data Protection Officer is easily accessible from each establishment.

7.5 Please describe any specific qualifications for the Data Protection Officer required by law.

The Data Protection Officer should be appointed on the basis of professional qualities and should have an expert knowledge of data protection law and practices. While this is not strictly defined, it is clear that the level of expertise required will depend on the circumstances. For example, the involvement of large volumes of sensitive personal data will require a higher level of knowledge.

7.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?

A Data Protection Officer should be involved in all issues which relate to the protection of personal data. The GDPR outlines the minimum tasks required by the Data Protection Officer, which include: (i) informing the controller, processor and their relevant employees who process data of their obligations under the GDPR; (ii) monitoring compliance with the GDPR, national data protection legislation and internal policies in relation to the processing of personal data including internal audits; (iii) advising on data protection impact assessments (“DPIA”) and the training of staff; and (iv) co-operating with the relevant data protection authority and acting as the authority’s primary contact point for issues related to data processing.

7.7 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?

Yes, the controller or processor must communicate the contact details of the Data Protection Officer to the NDPA. The NDPA has set up a registration system where organisations can register the contact details of the Data Protection Officer. Registration may be made online.

8.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?

Yes. The business that appoints a processor to process personal data on its behalf is required to enter into an agreement with the processor which sets out the subject matter for processing, the duration of processing, the nature and purpose of processing and the obligations and rights of the controller (i.e., the business) and of the processor. See further question 8.2.

It is essential that the processor appointed by the business complies with the GDPR.

8.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?

The processor must be appointed under a binding agreement in writing. The contractual terms must stipulate that the processor: (i) only acts on the documented instructions of the controller; (ii) imposes confidentiality obligations on all employees and others authorised to process personal data; (iii) ensures the security of personal data that it processes; (iv) abides by the rules regarding the appointment of sub-processors; (v) implements measures to assist the controller with guaranteeing the rights of data subjects; (vi) assists the controller in ensuring compliance with the controller’s obligations to ensure the security of personal data, the notification of a personal data breach, the carrying out of a DPIA and prior consultation; (vii) either returns or destroys the personal data at the end of the relationship (except as required by EU or Member State law); and (viii) provides the controller with all information necessary to demonstrate compliance with the GDPR.
9 Marketing

9.1 Please describe any legislative restrictions on the sending of electronic direct marketing (e.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?).

According to the Marketing Control Act, consumers may opt out of marketing by telephone or addressed mail by registering their names, addresses and telephone numbers in the Central Marketing Exclusion Register. Both consumers and other natural persons may opt out by contacting the trader directly. Telephone marketing on Saturdays, Sundays, public holidays or on weekdays before 09:00 or after 21:00 is prohibited.

Marketing communications may not be directed at natural persons during the course of trade (using electronic methods of communication which permit individual communication, such as electronic mail, telefax or automated calling systems) without the prior consent of the recipient. Such prior consent shall not, however, apply to marketing:

(a) where the natural person is contacted orally by telephone; or

(b) by means of electronic mail where there is an existing customer relationship and the contracting trader has obtained the electronic address of the customer in connection with a sale. The marketing may only relate to the trader’s own goods, services or other products corresponding to those on which the customer relationship is based. At the time that the electronic address is obtained, and at the time of any subsequent marketing communication, the customer shall be given a simple and free opportunity to opt out of receiving such communications.

9.2 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.).

With regard to telephone marketing, businesses cannot contact consumers who have opted out of marketing by registering in the Central Marketing Exclusion Register or contact natural persons who have opted out of such marketing directly with the trader unless:

(i) the natural person has made an express request to a specific trader concerning receiving such marketing from the trader (such request may be withdrawn at any time); or

(ii) in the case where consumers have opted out of marketing in the Central Marketing Exclusion Register, there is an existing customer or donor relationship and the trader has received the consumer’s contact information in connection with sales or fundraising. Such marketing can only relate to the trader’s own products that correspond to those on which the customer or donor relationship is based.

The same prohibitions and restrictions as those described in the preceding paragraph apply with regard to direct marketing by addressed mail.

Traders are obliged to update their address register in line with the Central Marketing Exclusion Register before their first inquiry, and before inquiry in the month when the marketing is conducted. Traders must also make sure that natural persons, easily and without costs, can opt out of marketing directly with the trader.

9.3 Do the restrictions noted above apply to marketing sent from other jurisdictions?

Yes, the Marketing Control Act applies to all actions and terms aimed at consumers or businesses in Norway.

9.4 Is/are the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?

No, compliance with the provisions of the Marketing Control Act, mentioned in questions 9.1 to 9.3 above, is monitored by the Consumer Authority (formerly known as the Consumer Ombudsman) and the Market Council.

9.5 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?

A marketing list from third parties may be used for telephone marketing and/or marketing by addressed mail provided that the conditions, restrictions and prohibitions specified in questions 9.1 and 9.2 are adhered to.

In practice, marketing lists from third parties can rarely satisfy the legal requirements for use for marketing via electronic methods of communication which permit individual communication (e.g., email, SMS) pursuant to section 15 of the Marketing Control Act. A marketing list from third parties cannot be used for marketing via electronic methods of communication which permit individual communication, unless the prior consent of the recipient (customer) for such type of direct marketing has been obtained beforehand. Such consent must be specific, informed, freely given and unambiguous. According to guidelines from the Consumer Authority, the requirement for informed consent means that, when consent is being collected, the consumer must have been informed about who the consent is being given to. If the consent is collected on behalf of an organisation’s business partners, this must be clearly indicated and there must be an updated list of names of all such business partners in the consent declaration, together with a description of the type of marketing that these will be sending and the extent thereof. Furthermore, such prior consent cannot be collected via electronic methods of communications such as email; i.e., a business cannot communicate via email or SMS with a consumer to ask whether he/she wishes to consent to marketing via email, SMS or other electronic method of communication falling within section 15 of the Marketing Control Act.

9.6 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?

The Consumer Council and the Market Council may impose an enforcement penalty (tvangsmulkt) or an infringement penalty (overtredelsesgebyr). When determining the amount of an enforcement penalty, which could take the form of a running charge or a lump sum, emphasis is given to the consideration that it must not be profitable to breach the decision of the Council or Market Council. In the determination of the amount of an infringement penalty, emphasis is given to the severity, scope and effects of the infringement.

10 Cookies

10.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).

The Electronic Communications Act of 25 July 2003, as amended with effect from 1 July 2013, regulates the use of cookies on websites in section 2-7 b. This act implements the requirements of

According to section 2-7 b of the Electronic Communications Act, the storage of data in the user’s communications equipment, or access thereto, is not permitted unless the user is informed of what data are processed, the purpose of the processing, who is processing the data; and unless the user has consented thereto. The aforesaid does not hinder technical storage of or access to data: (a) exclusively for the purpose of transmitting a communication in an electronic communications network; or (b) where the cookie is strictly necessary to provide an “information society service” (e.g., a service over the internet) requested by the subscriber or user, which means that it must be essential to fulfil their request.

The consent of the end user is a prerequisite for cookies to be used. As long as there is clear information available on the website itself about what cookies are used, which information is processed, the purpose of the processing and who is processing the data, consent may be given by the end user making use of a technical setting in the web browser or similar measure. A pre-setting in the web browser that the user accepts cookies is deemed to be consent. It is sufficient that the user consents once for the same purpose. The user must have the possibility to withdraw his/her consent.

10.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?

No, they do not.

10.3 To date, has/have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?

In 2015, the Norwegian Communications Authority initiated a review of Norwegian websites to determine how such websites are implementing the requirements of the aforementioned section 2-7 b. The Norwegian Communications Authority looked at the 500 most visited Norwegian websites. Four out of five of the investigated websites were found to be non-compliant. The Authority contacted the non-compliant websites and stated that it would re-examine the websites to verify compliance. No infringement penalties have been issued so far.

If there is refusal to abide by the information requirements, the sanction mechanisms in the law consist of the issue of an order to rectify one’s position and/or an infringement penalty.

10.4 What are the maximum penalties for breaches of applicable cookie restrictions?

Breach of section 2-7 b may give rise to an infringement penalty (overtredelsesgebyr); its extent depends on the seriousness and length of the infringement, the degree of fault and the turnover of the business. According to the Electronic Communications Regulations, in the case of wilful or negligent infringement, the amount may be up to 5% of the turnover, with turnover being the total sales revenue of the business for the last accounting year; where the infringer is a group of companies and the infringement concerns the group members’ activities, the turnover is the total sales revenue for the member firms that are active in the market affected by the infringement. Physical persons who wilfully or negligently infringe such provisions may incur an infringement penalty of up to 30 times the court fee (which at present is NOK 1,150); i.e., up to NOK 34,500.

According to section 12-4 of the Electronic Communications Act, wilful or negligent infringement may also give rise to criminal penalties punishable by the imposition of a fine or imprisonment for up to six months.

Where cookies are used for the processing of personal data in breach of the Personal Data Act, the sanction provisions in the Personal Data Act and the GDPR (see question 16.1) are applicable.

11 Restrictions on International Data Transfers

11.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.

Data transfers to other jurisdictions that are not within the EEA can only take place if the transfer is to an “Adequate Jurisdiction” (as specified by the EU Commission) or the business has implemented one of the required safeguards as specified by the GDPR.

11.2 Please describe the mechanisms businesses typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).

When transferring personal data to a country other than an Adequate Jurisdiction, businesses must ensure that there are appropriate safeguards on the data transfer as prescribed by the GDPR. The GDPR offers a number of ways to ensure compliance for international data transfers, one of which is consent of the relevant data subject. Other common options are the use of Standard Contractual Clauses or Binding Corporate Rules (“BCRs”).

Businesses can adopt the Standard Contractual Clauses drafted by the EU Commission – these are available for transfers between controllers, and transfers between a controller (as exporter) and a processor (as importer). International data transfers may also take place on the basis of contracts agreed between the data exporter and data importer, provided that they conform to the protections outlined in the GDPR and they have prior approval by the relevant data protection authority.

International data transfers within a group of businesses can be safeguarded by the implementation of BCRs. The BCRs will always need approval from the relevant data protection authority. Most importantly, the BCRs will need to include a mechanism to ensure they are legally binding and enforced by every member in the group of businesses. Among other things, the BCRs must set out the group structure of the businesses, the proposed data transfers and their purpose, the rights of data subjects, the mechanisms that will be implemented to ensure compliance with the GDPR, and the relevant complaint procedures.

Transfers of personal data to the US are also possible if the data importer has signed up to the EU-US Privacy Shield Framework, which was designed by the US Department of Commerce and the EU Commission to provide businesses in the EU and the US with a mechanism to comply with data protection requirements when transferring personal data from the EU to the US.
11.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.

It is likely that an international data transfer will require prior approval from the relevant data protection authority unless the controller or processor has already established a GDPR-compliant mechanism, as set out above, for such transfers.

In any case, most of the safeguards outlined in the GDPR, such as the establishment of BCRs, will need initial approval from the relevant data protection authority.

12 Whistle-blower Hotlines

12.1 What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?

Internal whistle-blowing schemes are generally established in pursuance of a concern to implement proper corporate governance principles in the daily functioning of businesses. Whistle-blowing is designed as an additional mechanism for employees to report misconduct internally through a specific channel, and supplements a business’s regular information and reporting channels, such as employee representatives, line management, quality-control personnel or internal auditors who are employed precisely to report such misconduct.

According to section 2 A-1 of the Working Environment Act, an employee has a right to notify censurable conditions at the employer’s undertaking. Workers hired from temporary-work agencies also have a right to notify censurable conditions at the hirer’s undertaking. According to section 2 A-3, if the conditions at the undertaking so indicate, the employer shall be obliged to prepare procedures for internal notification in connection with systematic health, environment and safety work. Such procedures must always be prepared if the undertaking regularly employs five or more employees. Such procedures shall be in writing and must, as a minimum, contain: (a) an encouragement to notify censurable conditions; (b) the procedure for notification; and (c) the procedure for receipt, processing and follow-up of notifications. The procedures must be easily accessible to all employees at the undertaking.

12.2 Is anonymous reporting prohibited, strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do businesses typically address this issue?

Anonymous reporting is not prohibited under EU data protection law; however, it raises problems as regards the essential requirement that personal data should only be collected fairly. As a rule, WP29 considers that only identified reports should be communicated through whistleblowing schemes in order to satisfy this requirement. WP29 holds that whistleblowing schemes should be built in such a way that they do not encourage anonymous reporting as the usual way to make a complaint.

According to section 2 A-4 of the Working Environment Act, when supervisory authorities or other public authorities receive notification concerning censurable conditions, any person who performs work or services for the body receiving such notification shall be obliged to prevent other persons from gaining knowledge of the employee’s name or other information identifying the employee. This duty of confidentiality also applies in relation to parties to the case (in connection with notification to public authorities) and their representative. However, it is to be noted that the duty of confidentiality does not apply with regard to the content of the notification – for example, factual data or a summary – if the conditions for access to information pursuant to the Freedom of Information Act or the Public Administration Act are otherwise fulfilled.

13 CCTV

13.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?

A DPIA must be undertaken with assistance from the Data Protection Officer when there is a systematic monitoring of a publicly accessible area on a large scale. If the DPIA suggests that the processing would result in a high risk to the rights and freedoms of individuals in the absence of measures taken to mitigate the risk, the controller must consult the data protection authority pursuant to Article 36 of the GDPR.

During the course of a consultation, the controller must provide information on the responsibilities of the controller and/or processors involved, the purpose of the intended processing, a copy of the DPIA, the safeguards provided by the GDPR to protect the rights and freedoms of data subjects and, where applicable, the contact details of the Data Protection Officer.

If the data protection authority is of the opinion that the CCTV monitoring would infringe the GDPR, it has to provide written advice to the controller within eight weeks of the request of a consultation and can use any of its wider investigative, advisory and corrective powers outlined in the GDPR.

The Personal Data Act has a provision regarding the use of fake camera surveillance. According to section 31, when camera surveillance is in breach of the GDPR or the Personal Data Act, it is also not permitted to use fake camera surveillance equipment or, by a sign, placard or similar, give the impression that there is camera surveillance. The term “camera surveillance” in section 31 is defined in the second paragraph as meaning continuous or regularly repeated surveillance of persons by means of a remote-controlled or automatically operated video camera or similar device, which is permanently fixed. “Fake camera surveillance” is defined as equipment which can easily be confused with real camera surveillance.

With regard to camera surveillance of employees, see section 14.

13.2 Are there limits on the purposes for which CCTV data may be used?

The GDPR does not have any specific provisions on CCTV. Thus, processing of personal data that occurs via CCTV is regulated by the GDPR’s general rules in Article 6. How the GDPR’s general rules will be applied with regard to the processing of personal data via CCTV, e.g., what constitutes the possibility of monitoring, deletion deadlines, notices, etc. will depend on further interpretation of the
GDPR. This, according to the preparatory works to the Personal Data Act, must be clarified through practice and perhaps through guidance from the supervisory authority.

In the preparatory works to the Personal Data Act, the Ministry of Justice stated that it is not at present necessary to provide provisions in national law which specifically make an exception from the prohibition in Article 9(1) for CCTV monitoring which has the purpose of capturing sensitive personal data.

With regard to camera surveillance of employees, see section 14.

14 Employee Monitoring

14.1 What types of employee monitoring are permitted (if any), and in what circumstances?

Specific provisions regarding employee monitoring, pursuant to GDPR Article 88, have been implemented as regulations to the Working Environment Act.

One set of such regulations to the Working Environment Act contain provisions regarding video surveillance in places of the employer’s undertaking that are frequented by a limited group of persons. Such video surveillance is subject to the general terms pursuant to the Working Environment Act chapter 9 on control measures in relation to employees, and is furthermore only permitted if, according to the activity, there is a need to prevent hazardous situations from arising and to protect the safety of employees or others, or if the surveillance is deemed essential for other reasons.

Another set of regulations to the Working Environment Act relate to the examination of employee emails. According to the regulations, an employer may only access email in an employee’s email account (a) when necessary to maintain daily operations or other justified interests of the business, or (b) in cases of justified suspicion that the employee’s use of email constitutes a serious breach of the duties that follow from the employment, or may constitute grounds for termination or dismissal. The aforementioned term “necessary” is interpreted restrictively. These provisions also apply to other personal workspaces in the undertaking’s communication network, and other electronic equipment provided by the employer.

14.2 Is consent or notice required? Describe how employers typically obtain consent or provide notice.

According to the regulations regarding video surveillance in the employer’s undertaking, attention must be drawn clearly, by means of a sign or in some other way, to the fact that a particular place is under surveillance, that the surveillance may include sound recordings, and to the identity of the controller.

According to the regulations regarding examination of employee emails, the employee shall be notified whenever possible and given an opportunity to speak before the employer makes any such examination. In the notice, the employer shall explain why the criteria mentioned above in question 14.1 are believed to be met, and shall advise on the employee’s rights. The employee shall, whenever possible, have the opportunity to be present during the examination, and has the right to the assistance of an elected employee representative or other representative. If the examination is made without prior warning, the employee shall receive subsequent written notification of the examination as soon as it is done.

14.3 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?

The general provisions in the Working Environment Act regarding control measures in relation to employees apply. Thus, an employer is, inter alia, obliged as early as possible to discuss needs, designs, implementation and major changes to control measures in the undertaking with the employees’ elected representatives.

See also question 14.2.

15 Data Security and Data Breach

15.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?

Yes. Personal data must be processed in a way that ensures security and safeguards against unauthorised or unlawful processing, accidental loss, destruction and damage of the data.

Both controllers and processors must ensure they have appropriate technical and organisational measures to meet the requirements of the GDPR. Depending on the security risk, this may include the encryption of personal data, the ability to ensure the ongoing confidentiality, integrity and resilience of processing systems, the ability to restore access to personal data following a technical or physical incident, and a process for regularly testing and evaluating the technical and organisational measures for ensuring the security of processing.

15.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

The controller is responsible for reporting a personal data breach without undue delay (and in any case within 72 hours of first becoming aware of the breach) to the relevant data protection authority, unless the breach is unlikely to result in a risk to the rights and freedoms of the data subject(s). A processor must notify any data breach to the controller without undue delay.

The notification must include the nature of the personal data breach, including the categories and number of data subjects concerned, the name and contact details of the Data Protection Officer or relevant point of contact, the likely consequences of the breach, and the measures taken to address the breach, including attempts to mitigate possible adverse effects.

15.3 Is there a legal requirement to report data breaches to affected data subjects? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

Controllers have a legal requirement to communicate the breach to the data subject, without undue delay, if the breach is likely to result in a high risk to the rights and freedoms of the data subject.
The notification must include the name and contact details of the Data Protection Officer (or point of contact), the likely consequences of the breach, and any measures taken to remedy or mitigate the breach.

The controller may be exempt from notifying the data subject if: the controller has implemented appropriate technical and organisational measures that render the personal data unintelligible (e.g., because the affected data is encrypted); the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialise; or the notification requires a disproportionate effort, in which case there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

Pursuant to section 16 of the Personal Data Act, the duty to notify the data subject does not apply to the extent such notification will reveal information: (i) that is of importance to Norway’s foreign political interests or national defence and security interests, when the controller can exempt such information pursuant to section 20 or section 21 of the Freedom of Information Act; (ii) that it is essential to keep secret for the purposes of preventing, investigating, revealing and judicial proceedings of criminal offences; and (iii) that, in statute or based on statute, is subject to confidentiality.

15.4 What are the maximum penalties for data security breaches?

The maximum penalty for breach of sections 32 to 34 of the GDPR is €10 million or 2% of worldwide turnover, whichever is higher.

16 Enforcement and Sanctions

16.1 Describe the enforcement powers of the data protection authority(ies).

<table>
<thead>
<tr>
<th>Investigatory Power</th>
<th>Civil/Administrative Sanction</th>
<th>Criminal Sanction</th>
</tr>
</thead>
<tbody>
<tr>
<td>Investigating Powers</td>
<td>The NDPA has wide powers to order the controller and the processor to provide any information it requires for the performance of its tasks, to conduct investigations in the form of data protection audits, to carry out reviews on certificates issued pursuant to the GDPR, to notify the controller or processor of alleged infringement of the GDPR, to access all personal data and all information necessary for the performance of controllers’ or processors’ tasks, and to access the premises of the data, including any data processing equipment.</td>
<td>N/A</td>
</tr>
<tr>
<td>Corrective Powers</td>
<td>The NDPA has a wide range of powers, including to issue warnings or reprimands for non-compliance, to order the controller to disclose a personal data breach to the data subject, to impose a permanent or temporary ban on processing, to withdraw a certification and to impose an administrative fine (as below).</td>
<td>N/A</td>
</tr>
<tr>
<td>Authorisation and Advisory Powers</td>
<td>The NDPA has a wide range of powers to advise the controller, accredit certification bodies and authorise certificates, contractual clauses, administrative arrangements and binding corporate rules as outlined in the GDPR.</td>
<td>N/A</td>
</tr>
</tbody>
</table>

16.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?

The GDPR entitles the relevant data protection authority to impose a temporary or definitive limitation, including a ban on processing.

16.3 Describe the data protection authority’s approach to exercising those powers, with examples of recent cases.

During 2018, the NDPA allocated a significant amount of time and resources to providing guidance and information to government bodies, private businesses and individuals on the main changes brought about by the GDPR.

The NDPR carried out 196 supervisions in 2018, all of them via written correspondence rather than physical inspections, so as to give the private and public sectors time to conform to the new legislation.

The NDPA received a record high number of cases, amounting to 2,654 new cases in 2018 (as opposed to 1,807 in 2017). A total of 246 individual decisions were given by the NDPA in 2018, which is significantly lower than previous years due to the fact that the GDPR removed the requirement to obtain prior approval/licence. A record 1,275 notifications of personal data breaches were made to the NDPA in 2018 (821 of which were made after the GDPR came into force).

Administrative fines were imposed in 13 cases and an enforcement penalty was imposed in one case. The penalties imposed by the NDPA have ranged from NOK 75,000 to NOK 800,000.

Towards the end of 2018, the NDPA gave Bergen municipality advance notice of its decision to impose an administrative fine amounting to NOK 1.6 million on the grounds that, because of inadequate technical and organisational measures to ensure information security, the personal data of a large amount of persons – in particular, children in the municipality’s primary schools – were at risk of unauthorised access. This case is still pending.

16.4 Does the data protection authority ever exercise its powers against businesses established in other jurisdictions? If so, how is this enforced?

For the time being, we have not seen any cases where the NDPA has exercised its powers against companies established in another jurisdiction.
17 E-discovery / Disclosure to Foreign Law Enforcement Agencies

17.1 How do businesses typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?

Unless there is an explicit legal basis for the requested transfer, such a transfer will probably be deemed to have a purpose which is incompatible with the original purpose for which the data had been collected, thereby necessitating consent from the data subject.

17.2 What guidance has/have the data protection authority(ies) issued?

The NDPA has not issued specific guidance on this issue.

18 Trends and Developments

18.1 What enforcement trends have emerged during the previous 12 months? Describe any relevant case law.

Before the entry into force of the new Personal Data Act and the GDPR on 20 July 2018, the NDPA was mostly engaged in a number of preparatory activities such as internal competence building, revision of the content on the NDPA’s website in light of the GDPR, and winding up of cases related to the previous data protection legislation. Since 20 July 2018, the NDPA has focused on, *inter alia*, analysing the personal breach notifications that have been filed, developing new and updating existing guidelines, and carrying out the first inspections under the new GDPR regime. The first inspections were centred around checking the extent to which public authorities or bodies had appointed a data protection officer. See also question 16.3 above.

18.2 What “hot topics” are currently a focus for the data protection regulator?

The main focus of the NDPA in 2018 was on the regulatory changes brought about by the GDPR. Most of its tasks revolved around guidance, as well as educational and other dissemination activities, regarding such changes.

An important “hot topic” is the development of artificial intelligence (AI) and robots; especially the security of such technology, its deployment in financial services, and the ethical implications of automated decisions made by various algorithms and AI systems.

Another key area is the increased use of Big Data and AI in the health care sector – both in the provision of primary health care as well as secondary use for research and quality assurance.
Line Coll is a Partner at Wikborg Rein’s Oslo office and Head of the firm’s Technology and Digitalisation team. Line specialises in privacy and digitalisation, and has more than 20 years’ practical experience as a lawyer within data protection law, privacy, the use of new technology and digitalisation, both as a business lawyer for a wide range of public and private Norwegian and international clients, as well as an in-house lawyer at Statoil ASA (Equinor ASA). Line has published books and articles on data protection and privacy, and is a frequent speaker at conferences.

She assists Norwegian and foreign clients in the public and private sectors, primarily with issues relating to privacy, data protection and e-commerce law.

Within the field of privacy and data protection, Ms. Coll has assisted Norwegian and international clients with General Data Protection Regulation (“GDPR”) compliance, providing strategic advice on both risk and approach, and on practical issues such as setting up internal control documentation and procedures, drafting data processor agreements, and privacy and cookie policies.

Emily M. Weitzenboeck has been active in the field of IT law for over 20 years, both as a practitioner and an academic. She is a Senior Lawyer at Wikborg Rein’s Oslo office and forms part of the firm’s Technology and Digitalisation team, and is an associate professor of law at Oslo Metropolitan University. At Wikborg Rein, she has assisted Norwegian and foreign clients in the public and private sectors, primarily with issues relating to privacy and data protection, e-commerce law, contract law including ICT contracts, marketing law and eHealth law.

Within the field of privacy and data protection, Dr. Weitzenboeck has assisted Norwegian and international clients with various questions related to GDPR compliance, and has drafted and quality-assured privacy policies and data processor agreements, etc.

Dr. Weitzenboeck was awarded a Ph.D. from the University of Oslo in 2010, has published several works and is a frequent speaker at conferences, as well as a lecturer and examiner at OsloMet, the Norwegian Research Centre for Computers and Law (University of Oslo) and the University of Malta.

WIKBORG REIN

Wikborg Rein is an international law firm with over 200 lawyers working in our offices in Oslo, Bergen, London, Singapore and Shanghai. Our unique and long-standing presence overseas enables us to offer our clients the benefit of our extensive international expertise.

Wikborg Rein’s broad range of legal services includes the following: corporate; dispute resolution; real estate and construction; labour law; banking and finance; shipping and offshore; energy and natural resources; public procurement; IPR; as well as data protection, digitalisation, information technology and telecommunications.

In the shipping and offshore fields, together with banking and finance, the firm is able to provide services under both Norwegian and English law. The firm has a dedicated team of tax lawyers with notable experience in cross-border taxation matters. In addition, the firm regularly advises on the application of European law, and on all aspects relevant to Norway’s position as a member of the EEA.
Chapter 36

Pakistan

S. U. Khan Associates
Corporate & Legal Consultants

1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

The legislation on data protection is in draft/Bill stage and yet to be passed by the Parliament. Its title is the Personal Data Protection Bill 2018 (“the Bill”).

1.2 Is there any other general legislation that impacts data protection?

The Prevention of Electronic Crimes Act, 2016 also contains certain significant provisions about data protection.

1.3 Is there any sector-specific legislation that impacts data protection?

Within the banking sector, the Payment Systems and Electronic Funds Transfers Act, 2007 provides for the secrecy of financial institutions’ customer information; violation is punishable with imprisonment or a financial fine, or both. For the telecoms industry, the Telecom Consumers Protection Regulations, 2009 confers on subscribers of telecoms operators the right to lodge complaints for any illegal practices with the Pakistan Telecommunication Authority, “illegal practices” being a broad term which includes, inter alia, illegal use of personal data of subscribers.

1.4 What authority(ies) are responsible for data protection?

Under the Bill, the proposed National Commission for Personal Data Protection would primarily be responsible for data protection.

2 Definitions

2.1 Please provide the key definitions used in the relevant legislation:

- “Personal Data”
  “Personal data” means any information in respect of commercial transactions, which:
  (i) is being processed wholly or partly by means of equipment operating automatically in response to instructions given for that purpose;
  (ii) is recorded with the intention that it should wholly or partly be processed by means of such equipment; or
  (iii) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system,
  that relates directly or indirectly to a data subject, who is identified or identifiable from that information or from that and other information in the possession of a data controller, including any sensitive personal data and expression of opinion about the data subject.

- “Processor”
  “Data processor”, in relation to personal data, means any person, other than an employee of the data user, who processes the personal data solely on behalf of the data controller, and does not process the personal data for any of his own purposes.

- “Controller”
  “Data controller” means a person who either alone or jointly or in common with other persons processes any personal data or has control over or authorises the processing of any personal data, but does not include a data processor.

- “Processing”
  “Processing”, in relation to personal data, means collecting, recording, holding or storing the personal data or carrying out any operation or set of operations on the personal data, including:
  (i) the organisation, adaptation or alteration of personal data;
  (ii) the retrieval, consultation or use of personal data; and
  (iii) the disclosure of personal data by transmission, transfer, dissemination or otherwise making available; or
  (iv) the alignment, combination, correction, erasure or destruction of personal data.

- “Data Subject”
  “Data subject” means an individual who is the subject of the personal data.

- “Sensitive Personal Data”
  “Sensitive personal data” means personal data revealing racial or ethnic origin, religious, philosophical or other beliefs, political opinions, membership in political parties, trade unions, organisations and associations with a religious, philosophical, political or trade-union, or provide information as to the health or sexual life of an individual, or the commission or alleged commission by him of any offence, or any proceedings for any offence committed or alleged to have
been committed by him, or the disposal of such proceedings or the sentence of any court in such proceedings or financial, or proprietary confidential personal data; OR “sensitive personal data” means any personal data consisting of information as to the physical or mental health or condition of a data subject, his political opinions, his religious beliefs or other beliefs of a similar nature, the commission or alleged commission by him of any offence or any other personal data as the Commission may determine by order published in the Gazette.

■ “Data Breach”
There is no definition of this term in the relevant national legislation.

■ Other key definitions – please specify (e.g., “Pseudonymous Data”, “Direct Personal Data”, “Indirect Personal Data”)
“Commercial transaction” means any transaction of a commercial nature, whether contractual or not, which includes any matters relating to the supply or exchange of goods or services, agency, investments, financing, banking and insurance. “Vital interests” means matters relating to life, death or security of a data subject.

3 Territorial Scope

3.1 Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to those laws?
Section 3(2)(b) of the Bill brought the applicability of the Bill on businesses (persons) not established in Pakistan but using equipment in Pakistan for processing personal data otherwise than for the purposes of transit through Pakistan. Those persons are required to nominate a representative in Pakistan for the purposes of the Bill.

4 Key Principles

4.1 What are the key principles that apply to the processing of personal data?
■ Transparency
The principle of transparency is not dealt with in the Bill.

■ Lawful basis for processing
Personal data shall not be processed unless the personal data are processed for a lawful purpose directly related to an activity of the data controller.

■ Purpose limitation
Personal data shall not be processed unless the processing of the personal data is necessary for or directly related to that purpose.

■ Data minimisation
Personal data shall not be processed unless the personal data are adequate but not excessive in relation to that purpose.

■ Proportionality
This is not dealt with in the Bill.

■ Retention
The Bill stipulates that personal data processed for any purpose shall not be kept longer than is necessary for the fulfilment of that purpose. The Bill confers a duty on the data controller to take all reasonable steps to ensure that all personal data are destroyed or permanently deleted if they are no longer required for the purpose for which they were to be processed.

■ Other key principles – please specify
The Bill recognises and provides for consent to be an essential requirement to process personal data of the data subject. The Bill also provides that the data controller may not disclose personal data without the consent of the data subject. The data controller is further required to take practical steps to protect the personal data from any loss, misuse, modification, unauthorised or accidental access or disclosure, alteration or destruction.

5 Individual Rights

5.1 What are the key rights that individuals have in relation to the processing of their personal data?

■ Right of access to data/copies of data
The data subject is granted the right of access to personal data, upon payment of a prescribed fee, and the data controller with information as to the data subject’s personal data that are being processed by or on behalf of the data controller, must comply with such data access request within 21 days. The data subject is entitled to:
  ■ information as to the data subject’s personal data that are being processed by or on behalf of the data controller; and
  ■ have communicated to him a copy of the personal data in an intelligible form.

■ Right to rectification of errors
In the case that personal data have been supplied to the data subject upon his request and the same is inaccurate, incomplete, misleading or not up to date, or when the data subject knows that his personal data are so inaccurate, incomplete, misleading or not up to date, the data subject has the right to get it corrected by making a written request to the data controller.

■ Right to deletion/right to be forgotten
The data subject has the right to request that the data controller, without undue delay, erase personal data in the following situations:
  ■ the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
  ■ the data subject withdraws consent on which the processing is based;
  ■ the data subject objects to the processing;
  ■ the personal data have been unlawfully processed; or
  ■ the personal data have to be erased for compliance with a legal obligation.

■ Right to object to processing
The data subject has the right to give “data subject notice” in writing to the data controller to:
(i) cease the processing, or processing for a specified purpose, or in a specified manner; or
(ii) not begin the processing, or processing for a specified purpose, or in a specified manner.

The data subject has to state reasons in the “data subject notice” that:
(i) the processing of that personal data or the processing of personal data for that purpose or in that manner is causing or is likely to cause substantial damage or substantial distress to him or to another person; and
(ii) the damage or distress is or would be unwarranted.

■ Right to restrict processing
As explained above.
Right to data portability
There is no such right in the Bill.

Right to withdraw consent
The data subject has the right to withdraw his consent.

Right to object to marketing
The data subject has the right to give “data subject notice” in writing to the data controller to:
(i) cease the processing of the data or their processing for a specified purpose or in a specified manner; or
(ii) not begin the processing of the data or their processing for a specified purpose, or in a specified manner.
The data subject has to state reasons in the “data subject notice” that:
(i) the processing of that personal data or the processing of personal data for that purpose or in that manner is causing or is likely to cause substantial damage or substantial distress to him or to another person; and
(ii) the damage or distress is or would be unwarranted.

Right to complain to the relevant data protection authority(ies)
The data subject may file a complaint before the National Commission for Personal Data Protection against any violation of personal data protection rights as granted under the Bill, regarding the conduct of any data controller, data processor or their processes which the data subject regards as involving:
(i) a breach of data subject’s consent to process data;
(ii) a breach of obligations of the data controller or the data processor in the performance of their functions under the Bill;
(iii) the provision of incomplete, misleading or false information while taking consent of the data subject; or
(iv) any other matter relating to protection of personal data.

Other key rights – please specify
None other than the above.

6 Registration Formalities and Prior Approval

6.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?
There are no such requirements in the Bill; however, the Bill confers upon the Federal Government powers for rule-making. It is expected that after the promulgation of the law, the Federal Government, in the exercise of its rule-making powers, will notify such procedural requirements.

6.2 If such registration/notification is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?
This aspect will be addressed under the rules to be framed by the Federal Government (please see question 6.1 above).

6.3 On what basis are registrations/notifications made (e.g., per legal entity, per processing purpose, per data category, per system or database)?
This aspect will be addressed under the rules to be framed by the Federal Government (please see question 6.1 above).

6.4 Who must register with/notify the data protection authority (e.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation)?
This aspect will be addressed under the rules to be framed by the Federal Government (please see question 6.1 above).

6.5 What information must be included in the registration/notification (e.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes)?
This aspect will be addressed under the rules to be framed by the Federal Government (please see question 6.1 above).

6.6 What are the sanctions for failure to register/notify where required?
This aspect will be addressed under the rules to be framed by the Federal Government (please see question 6.1 above).

6.7 What is the fee per registration/notification (if applicable)?
This aspect will be addressed under the rules to be framed by the Federal Government (please see question 6.1 above).

6.8 How frequently must registrations/notifications be renewed (if applicable)?
This aspect will be addressed under the rules to be framed by the Federal Government (please see question 6.1 above).

6.9 Is any prior approval required from the data protection regulator?
This aspect will be addressed under the rules to be framed by the Federal Government (please see question 6.1 above).

6.10 Can the registration/notification be completed online?
This aspect will be addressed under the rules to be framed by the Federal Government (please see question 6.1 above).

6.11 Is there a publicly available list of completed registrations/notifications?
This aspect will be addressed under the rules to be framed by the Federal Government (please see question 6.1 above).
6.12 How long does a typical registration/notification process take?

This aspect will be addressed under the rules to be framed by the Federal Government (please see question 6.1 above).

7 Appointment of a Data Protection Officer

7.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.

The Bill does not have a requirement for the appointment of a Data Protection Officer, either mandatory or optional.

7.2 What are the sanctions for failing to appoint a Data Protection Officer where required?

In view of question 7.1 above, this is not applicable.

7.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect of his or her role as a Data Protection Officer?

In view of question 7.1 above, this is not applicable.

7.4 Can a business appoint a single Data Protection Officer to cover multiple entities?

In view of question 7.1 above, this is not applicable.

7.5 Please describe any specific qualifications for the Data Protection Officer required by law.

In view of question 7.1 above, this is not applicable.

7.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?

In view of question 7.1 above, this is not applicable.

7.7 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?

In view of question 7.1 above, this is not applicable.

7.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?

In view of question 7.1 above, this is not applicable.

8 Appointment of Processors

8.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?

The Bill is silent on this aspect; however, businesses customarily execute an agreement to this effect.

8.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?

It is not necessary, under the Bill, to enter into an agreement. However, for the enforcement of an agreement, such formalities need to be summarised in writing and registered under the Registration Act, 1908.

9 Marketing

9.1 Please describe any legislative restrictions on the sending of electronic direct marketing (e.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?).

No such legislative restriction exists.

9.2 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.).

No such legislative restriction exists.

9.3 Do the restrictions noted above apply to marketing sent from other jurisdictions?

No such legislative restriction exists.

9.4 Is/are the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?

A data protection authority, for the time being, is non-existent.

9.5 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?

There is no law regulating this mechanism as such.

9.6 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?

There are none, as there is no legislation to this effect.
## 10 Cookies

### 10.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).

No such legislative restriction exists.

### 10.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?

No such legislative restriction exists.

### 10.3 To date, has/have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?

None, in view of there not being any legislation to this effect, and the fact that no data protection authority exists.

### 10.4 What are the maximum penalties for breaches of applicable cookie restrictions?

None, in view of there not being any legislation to this effect.

## 11 Restrictions on International Data Transfers

### 11.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.

No such legislative restriction exists.

### 11.2 Please describe the mechanisms businesses typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).

There are no such mechanisms, in view of there not being any legislation to this effect.

### 11.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.

This is not required, as there is no legislation to this effect.

## 12 Whistle-blower Hotlines

### 12.1 What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?

The Public Interest Disclosures Act, 2017 deals with the concept of “whistle-blowers”; however, the same primarily deals with and focuses on public sector entities. The said Act has mandated the Government to specify private sector entities (in the official Gazette) to be an “organization” for the purposes of the said Act. Primarily, the Public Interest Disclosures Act, 2017 covers the wilful misuse of power or wilful misuse of discretion by virtue of which substantial loss is caused to the Government or substantial wrongful gain accrues to a public servant or to a third party. As such, the corporate sector is not the subject matter of the Public Interest Disclosures Act, 2017.

### 12.2 Is anonymous reporting prohibited, strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do businesses typically address this issue?

Anonymous or pseudonymous disclosures are not entertained in terms of Section 3(5) of the Public Interest Disclosures Act, 2017.

## 13 CCTV

### 13.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?

There exists no legislation that requires registration/notification or prior approval for using CCTV.

### 13.2 Are there limits on the purposes for which CCTV data may be used?

There are no such limits (please see question 13.1 above).

## 14 Employee Monitoring

### 14.1 What types of employee monitoring are permitted (if any), and in what circumstances?

There is no law related to this subject.

### 14.2 Is consent or notice required? Describe how employers typically obtain consent or provide notice.

As there is no law, there is no legislative requirement to obtain consent; however, consent is generally built-in within the employment contract.
14.3 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?

There is no such requirement.

15 Data Security and Data Breach

15.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?

Data controllers, under the Bill, are responsible for taking practical steps to protect the personal data from any loss, misuse, modification, unauthorised or accidental access or disclosure, alteration or destruction.

15.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

The National Commission for Personal Data Protection has powers to seek information from the data controller in respect of data processing; however, as the said Commission is not yet in existence, there have not been any rules issued on this matter.

15.3 Is there a legal requirement to report data breaches to affected data subjects? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

There is no such requirement in the Bill.

15.4 What are the maximum penalties for data security breaches?

The National Commission for Personal Data Protection has powers to impose penalties for non-compliance and non-observance of data security practices; however, as the said Commission is not yet in existence, there is no quantification of such penalties.

16 Enforcement and Sanctions

16.1 Describe the enforcement powers of the data protection authority(ies).

<table>
<thead>
<tr>
<th>Investigatory Power</th>
<th>Civil/Administrative Sanction</th>
<th>Criminal Sanction</th>
</tr>
</thead>
<tbody>
<tr>
<td>Complaint redressal</td>
<td>To seek information from data controllers.</td>
<td>Direction to local police to file a case with the Court.</td>
</tr>
<tr>
<td>N/A</td>
<td>Imposition of penalties.</td>
<td>N/A</td>
</tr>
<tr>
<td>N/A</td>
<td>To order a data controller to take such reasonable measures as it may deem necessary to remedy an applicant for any failure to implement the provisions of the Bill.</td>
<td>N/A</td>
</tr>
</tbody>
</table>

16.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?

The National Commission for Personal Data Protection has powers to order a data controller to take such reasonable measures as it may deem necessary, which may include a ban; however, as the said Commission is not in existence, procedural aspects in relation to having an order from the Court, etc., are uncertain at the moment.

16.3 Describe the data protection authority’s approach to exercising those powers, with examples of recent cases.

As the National Commission for Personal Data Protection is not in existence, there is nothing to state regarding its approach, nor any cases as yet.

16.4 Does the data protection authority ever exercise its powers against businesses established in other jurisdictions? If so, how is this enforced?

This is not applicable (please see question 16.3 above).

17 E-discovery / Disclosure to Foreign Law Enforcement Agencies

17.1 How do businesses typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?

The Bill is silent on this aspect; however, generally the foreign law enforcement agencies do not communicate with businesses directly; rather, businesses are contacted via the relevant law enforcement agencies of Pakistan, who coordinate with businesses to respond to foreign law enforcement agencies.
17.2 What guidance has/have the data protection authority(ies) issued?

No such guidelines exist.

18 Trends and Developments

18.1 What enforcement trends have emerged during the previous 12 months? Describe any relevant case law.

Recently, Pakistani bank data were the subject of a cyber attack, with customers receiving notification about money transfers from their account. Following various abnormal international transactions and complaints from customers, the affected bank immediately reacted and shut down its system to stop further transactions. This timely action helped keep losses to Rs 2.6m as opposed to Rs 5m to 6m. Currently, the State Bank of Pakistan and relevant agencies are investigating the incident. Pakistan’s Prevention of Electronic Crime Act, 2016 has already made unauthorised interference with information systems and transmission of data a criminal offence. Moreover, the State Bank of Pakistan has directed all banks to take steps to identify and counter any cyber threat to their IT systems in coordination with international payment schemes.

18.2 What “hot topics” are currently a focus for the data protection regulator?

As stated above, a National Commission for Personal Data Protection is not existent for the time being; however, once it comes into being, e-commerce, banking transactions and cellular data are certainly among the “hot topics” on which the said Commission is expected to focus.
Chapter 37

Portugal

Sónia Queiróz Vaz

Ana Costa Teixeira

1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

Since 25 May 2018, the main data protection legislation in the EU has been Regulation (EU) 2016/679 (the “General Data Protection Regulation” or “GDPR”). The GDPR repealed Directive 95/46/EC (the “Data Protection Directive”) and has led to increased (though not total) harmonisation of data protection law across the EU Member States.

Although Law no. 67/98 of 26 October (“Data Protection Act”), which transposed the Data Protection Directive, is still in force, it will be revoked once the new data protection law is approved by the Portuguese Parliament and enters into force.

1.2 Is there any other general legislation that impacts data protection?

There are other laws in Portugal, which impact data protection, for example:

- Constitution of the Portuguese Republic – Article 35 (use of computerised data);
- Regulation no. 1093/2016, of 14 December, which regulates the use of drones;
- Decree-Law no. 298/92, of 31 December, General Regime of Credit Institutions and Financial Companies; and
- Law no. 83/2017, of 18 August, containing measures to combat money laundering and the financing of terrorism.

1.3 Is there any sector-specific legislation that impacts data protection?

The Portuguese health, labour, banking and insurance sectors are subject to additional and specific statutory restrictions in relation to data protection.

1.4 What authority(ies) are responsible for data protection?

The Data Protection Act has created the Comissão Nacional de Protecção de Dados – the Portuguese Data Protection Authority (“CNPD”) – as the empowered body to supervise and monitor the compliance with laws and regulations within personal data protection.

2 Definitions

2.1 Please provide the key definitions used in the relevant legislation:

- “Personal Data” means any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

- “Processing” means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

- “Controller” means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. Where the purposes and means of such processing are determined by European Union or Member State law, the controller or the specific criteria for its nomination may be provided for by European Union or Member State law.

- “Processor” means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

- “Data Subject” means an individual who is the subject of the relevant personal data and who is an identifiable person who can be identified, directly or indirectly, in particular with reference to an indication number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.


3 Territorial Scope

3.1 Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to those laws?

The GDPR applies to businesses that are established in the EU and that process personal data (either as a controller or processor, and regardless of whether or not the processing takes place in the EU) in the context of that establishment.

A business that is not established in the EU, but is subject to the laws of a Member State by virtue of public international law, is also subject to the GDPR.

The GDPR applies to businesses outside the EU if they process the personal data of EU residents in relation to: (i) the offering of goods or services (whether or not in return for payment) to EU residents; or (ii) the monitoring of the behaviour of EU residents (to the extent that such behaviour takes place in the EU).

Further, the GDPR applies to businesses established outside the EU if they monitor the behaviour of EU residents (to the extent such behaviour takes place in the EU).

4 Key Principles

4.1 What are the key principles that apply to the processing of personal data?

- **Transparency**
  
  Personal data must be processed lawfully, fairly and in a transparent manner. Controllers must provide certain minimum information to data subjects regarding the collection and further processing of their personal data in a concise, transparent, intelligible and easily accessible form (using clear and plain language).

- **Lawful basis for processing**

  Processing of personal data is lawful only if, and to the extent that, it is permitted under EU data protection law. The GDPR provides an exhaustive list of legal bases on which personal data may be processed, of which the following are the most relevant: (i) prior, freely given, specific, informed and unambiguous consent of the data subject; (ii) contractual necessity (i.e., the processing is necessary for the performance of a contract to which the data subject is a party, or for the purposes of pre-contractual measures taken at the data subject’s request); (iii) compliance with legal obligations; or (iv) legitimate interests (i.e., the processing is necessary for the purposes of legitimate interests pursued by the controller, except where the controller’s interest are overridden by the interests, fundamental rights or freedoms of the affected data subjects).

Please note that businesses require stronger grounds to process special categories of personal data. Processing of these data is only permitted under certain conditions, of which the most relevant are: (i) explicit consent of the affected data subject; (ii) the processing is necessary in the context of employment law; or (iii) the processing is necessary for the establishment, exercise or defence of legal claims.

- **Purpose limitation**

  Personal data may only be collected for specified, explicit and legitimate purposes and must not be further processed in a manner that is incompatible with those purposes. If a controller wishes to use the relevant personal data in a manner that is incompatible with the purposes for which they were initially collected, it must: (i) inform the data subject of such new processing; and (ii) must be able to rely on a lawful basis as set out above.

- **Data minimisation**

  Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which those data are processed. A business should only process the personal data that it actually needs to process in order to achieve its processing purposes.

- **Proportionality**

  The processing of personal data should be designed to serve mankind. The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality.

- **Retention**

  Personal data must be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. Personal data may be stored for longer periods for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

**Other key principles – please specify**

- **Accuracy**

  Personal data must be accurate and, where necessary, kept up to date. A business must take every reasonable step to ensure that personal data that are inaccurate are either erased or rectified without delay.

- **Data security**

  Personal data must be processed in a manner that ensures appropriate security of those data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

- **Accountability**

  The controller is responsible for, and must be able to demonstrate, compliance with the data protection principles set out above.

5 Individual Rights

5.1 What are the key rights that individuals have in relation to the processing of their personal data?

- **Right of access to data/copies of data**

  A data subject has the right to obtain from a controller the following information in respect of the data subject’s personal data: (i) confirmation of whether, and where, the controller is processing the data subject’s personal data; (ii) information about the purposes of the processing; (iii)
Is there a legal obligation on businesses to register

Registration Formalities and Prior Approval

6.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?

Prior to the GDPR, the controller was obliged to notify or to file an authorisation request before the CNPD before carrying out a personal data processing operation. While that obligation produced administrative and financial burdens, it did not contribute to improving the protection of personal data. With the GDPR, this obligation has been abolished and replaced with effective procedures and mechanisms (data protection impact assessment (“DPIA”)), which focus on the processing operations that are likely to result in a high risk to the rights and freedoms of data subjects by virtue of their nature, scope, context and purposes. Recently, the CNPD published a list of personal data processing activities subject to DPIA in addition to those already exemplified in the GDPR. Nevertheless, the GDPR sets forth new obligations to notify the competent supervisory authority, for example in the case of a personal data breach.

6.2 If such registration/notification is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?

This is not applicable; please see question 6.1 above.
6.3 On what basis are registrations/notifications made (e.g., per legal entity, per processing purpose, per data category, per system or database)?

This is not applicable; please see question 6.1 above.

6.4 Who must register with/notify the data protection authority (e.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation)?

This is not applicable; please see question 6.1 above.

6.5 What information must be included in the registration/notification (e.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes)?

This is not applicable; please see question 6.1 above.

6.6 What are the sanctions for failure to register/notify where required?

This is not applicable; please see question 6.1 above.

6.7 What is the fee per registration/notification (if applicable)?

This is not applicable; please see question 6.1 above.

6.8 How frequently must registrations/notifications be renewed (if applicable)?

This is not applicable; please see question 6.1 above.

6.9 Is any prior approval required from the data protection regulator?

This is not applicable; please see question 6.1 above.

6.10 Can the registration/notification be completed online?

This is not applicable; please see question 6.1 above.

6.11 Is there a publicly available list of completed registrations/notifications?

Yes. The notifications and authorisations granted by the CNPD before the entry into force of the GDPR are available on the CNPD website.

6.12 How long does a typical registration/notification process take?

This is not applicable; please see question 6.1 above.

7 Appointment of a Data Protection Officer

7.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.

The appointment of a Data Protection Officer for controllers or processors is only mandatory in some circumstances, including where:

a. the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;

b. the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or

c. the core activities of the controller or the processor consist of processing on a large scale of special categories of data and personal data relating to criminal convictions and offences.

Where a business designates a Data Protection Officer voluntarily, the requirements of the GDPR apply as though the appointment were mandatory.

7.2 What are the sanctions for failing to appoint a Data Protection Officer where required?

Infringements of the following provisions shall be subject to administrative fines of up to €10,000,000, or in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

7.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect of his or her role as a Data Protection Officer?

The appointed Data Protection Officer should not be dismissed or penalised for performing their tasks and should report directly to the highest management level of the controller or processor.

7.4 Can a business appoint a single Data Protection Officer to cover multiple entities?

A single Data Protection Officer is permitted by a group of undertakings, provided that the Data Protection Officer is easily accessible from each establishment.

7.5 Please describe any specific qualifications for the Data Protection Officer required by law.

The Data Protection Officer should be appointed on the basis of professional qualities and should have an expert knowledge of data protection law and practices. While this is not strictly defined, it is clear that the level of expertise required will depend on the circumstances. For example, the involvement of large volumes of sensitive personal data will require a higher level of knowledge.

7.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?

A Data Protection Officer should be involved in all issues which relate to the protection of personal data. The GDPR outlines the
minimum tasks required by the Data Protection Officer, which include: (i) informing the controller, processor and their relevant employees who process data of their obligations under the GDPR; (ii) monitoring compliance with the GDPR, national data protection legislation and internal policies in relation to the processing of personal data including internal audits; (iii) advising on DPIAs and the training of staff; (iv) co-operating with the data protection authority; and (v) acting as the authority’s primary contact point for issues related to data processing.

7.7 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?

Yes, the controller or processor must notify the data protection authority of the contact details of the designated Data Protection Officer. In Portugal, an official notification form has been approved by the CNPD and can be filed directly online.

7.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?

The Data Protection Officer does not necessarily need to be named in the public-facing privacy notice. However, the contact details of the Data Protection Officer must be notified to the data subject when personal data relating to that data subject are collected. As a matter of good practice, the Article 29 Working Party (the “WP29”) (now the European Data Protection Board (the “EDPB”)) recommended in its 2017 guidance on Data Protection Officers that both the data protection authority and employees should be notified of the name and contact details of the Data Protection Officer.

8 Appointment of Processors

8.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?

Yes. The business that appoints a processor to process personal data on its behalf, is required to enter into an agreement with the processor which sets out the subject matter for the processing, its duration, its nature and purpose, the types of personal data and categories of data subjects and the obligations and rights of the controller (i.e., the business).

It is essential that the processor appointed by the business complies with the GDPR.

8.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?

The processor must be appointed under a binding agreement in writing, including in electronic form. The contractual terms must stipulate that the processor: (i) only acts on the documented instructions of the controller; (ii) imposes confidentiality obligations on all employees; (iii) ensures the security of personal data that it processes; (iv) abides by the rules of regarding the appointment of sub-processors; (v) implements measures to assist the controller with guaranteeing the rights of data subjects; (vi) assists the controller in obtaining approval from the relevant data protection authority; (vii) either returns or destroys the personal data at the end of the relationship (except as required by EU or Member State law); and (viii) provides the controller with all information necessary to demonstrate compliance with the GDPR.

9 Marketing

9.1 Please describe any legislative restrictions on the sending of electronic direct marketing (e.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?).

Under Law no. 41/2004 of 18 August (following the amendment of Law no. 46/2012 of 29 August), sending unrequested communications for direct marketing purposes requires the express prior consent of the subscriber or user (“opt-in”). This includes the use of automated calling and communication that do not rely on human intervention (automatic call devices), facsimile or electronic mail, including SMS, EMS, MMS and other similar applications. Nevertheless, if the above-mentioned communications refer to products or services similar to those which the data subject has already purchased from the controller, prior consent is not required, provided that he/she is able to oppose to such communications, both at the time of collection and at the time of sending each message (“opt-out”).

Although the “opt-in” rule does not apply to legal entities, Law no. 41/2004 also sets forth the right to “opt-out” for these entities. With the GDPR, the consent acquires a new relevance, namely in the marketing sector. As such, any organisation that wants to collect data must communicate clearly to the data subject what data is going to be used for. The data subjects will need to give their consent to that use and the consent needs to be clear, “informed, specific, unambiguous, and revocable”. Data subjects also need to be informed about their right to withdraw consent.

9.2 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.).

It is incumbent upon the Directorate General of Consumers (“DGC”) to keep up to date a national list of legal persons that expressly object to the receipt of unsolicited communications for direct marketing purposes. The entities that promote the sending of communications for direct marketing purposes are obliged to consult the list, updated monthly by the DGC, which is available on request.

Where the prior express consent of the subscriber (data subject) has been collected, such consent overrides the need to consult the above-referenced list.

9.3 Do the restrictions noted above apply to marketing sent from other jurisdictions?

The GDPR applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the EU, regardless of whether the processing takes place in the EU or not, including the following circumstances where the controller or processor are not established in the EU: (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the EU; or (b) the monitoring of their behaviour as far as their behaviour takes place within the European Union.
9.4 Is/are the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?

Although the CNPD is not very proactive in the execution of its supervision and monitoring powers, following a complaint, they are quick to open investigations and issue decisions.

9.5 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?

Consent requests must be prominent, unbundled from other terms and conditions, concise and easy to understand, user-friendly and must specifically cover the controller’s name, the purposes of the processing and the types of processing activity. As such, if the consent collected by the controller does not specifically cover third parties (with whom the controller may share consent) and the specific purposes for which these third parties will process the personal data shared, the sharing and/or acquisition of data for marketing purposes is unlawful.

9.6 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?

The CNPD and ICP-ANACOM are empowered to issue fines of up to €5 million and to seize any equipment, devices, or materials used to commit the infraction. Delays in complying with any orders or requests from the CNPD or ICP-ANACOM may also attract a fine of up to €100,000 for each day up to a maximum of €3 million (30 days’ delay).

When applicable, according to the GDPR a fine of up to €20 million or, in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher, can be issued.

10 Cookies

10.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).

Law no. 41/2004 of 18 August (following the amendment of Law no. 46/2012 of 29 August), which implements Article 5 of the ePrivacy Directive, determines that the storage of cookies (or other data) on an end user’s device requires prior consent (the applicable standard of consent is derived from the GDPR). For consent to be valid, it must be informed, specific, freely given and must constitute a real and unambiguous indication of the individual’s wishes. This does not apply if: (i) the cookie is for the sole purpose of carrying out the transmission of a communication over an electronic communications network; or (ii) the cookie is strictly necessary to provide an “information service” (e.g., a service over the internet) requested by the subscriber or user, which means that it must be essential to fulfil their request.

The EU Commission intends to pass a new ePrivacy Regulation that will replace the respective national legislation in the EU Member States. The ePrivacy Regulation is planned to come into force in 2019.

10.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?

Law no. 41/2004 of 18 August does not distinguish between different kinds of cookies. In order to determine whether the prior informed consent of users is required or not, the WP29 guidance on “cookie consent exemption” must be taken into consideration.

10.3 To date, has/have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?

To date, the CNPD has not taken any enforcement action in relation to cookies.

10.4 What are the maximum penalties for breaches of applicable cookie restrictions?

The CNPD and ICP-ANACOM are empowered to issue fines of up to €5 million and to seize any equipment, devices or materials used to commit the infraction. Delays in complying with any orders or requests from the CNPD or ICP-ANACOM may also attract a fine of up to €100,000 for each day up to a maximum of €3 million (30 days’ delay).

11 Restrictions on International Data Transfers

11.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.

Data transfers to other jurisdictions that are not within the European Economic Area (the “EEA”) can only take place if the transfer is to an “Adequate Jurisdiction” (as specified by the EU Commission), the business has implemented one of the required safeguards as specified by the GDPR, or one of the derogations specified in the GDPR applies to the relevant transfer. The EDPB Guidelines (2/2018) set out that a “layered approach” should be taken with respect to these transfer mechanisms. If the transfer is not to an Adequate Jurisdiction, the data exporter should first explore the possibility of implementing one of the safeguards provided for in the GDPR before relying on a derogation.

11.2 Please describe the mechanisms businesses typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).

When transferring personal data to a country other than an Adequate Jurisdiction, businesses must ensure that there are appropriate safeguards on the data transfer, as prescribed by the GDPR. The GDPR offers a number of ways to ensure compliance for international data transfers, of which one is consent of the relevant data subject. Other common options are the use of Standard Contractual Clauses or Binding Corporate Rules (“BCRs”).
Businesses can adopt the Standard Contractual Clauses drafted by the EU Commission – these are available for transfers between controllers, and transfers between a controller (as exporter) and a processor (as importer). International data transfers may also take place on the basis of contracts agreed between the data exporter and data importer provided that they conform to the protections outlined in the GDPR, and they have prior approval by the relevant data protection authority.

International data transfers within a group of businesses can be safeguarded by the implementation of BCRs. The BCRs will always need approval from the relevant data protection authority. Most importantly, the BCRs will need to include a mechanism to ensure they are legally binding and enforced by every member in the group of businesses. Among other things, the BCRs must set out the group structure of the businesses, the proposed data transfers and their purpose, the rights of data subjects, the mechanisms that will be implemented to ensure compliance with the GDPR and the relevant complainant procedures.

Transfer of personal data to the USA is also possible if the data importer has signed up to the EU-US Privacy Shield Framework, which was designed by the US Department of Commerce and the EU Commission to provide businesses in the EU and the US with a mechanism to comply with data protection requirements when transferring personal data from the EU to the US.

11.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.

It is likely that the international data transfer will require prior approval from the relevant data protection authority unless they have already established a GDPR-compliant mechanism as set out above for such transfers.

In any case, most of the safeguards outlined in the GDPR will need initial approval from the data protection authority, such as the establishment of BCRs.

12 Whistle-blower Hotlines

12.1 What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?

Internal whistle-blowing schemes are generally established in pursuance of a concern to implement proper corporate governance principles in the daily functioning of businesses. Whistle-blowing is designed as an additional mechanism for employees to report misconduct internally through a specific channel and supplements a business’ regular information and reporting channels, such as employee representatives, line management, quality-control personnel or internal auditors who are employed precisely to report such misconduct.

The WP29 has limited its Opinion 1/2006 on the application of EU data protection rules to internal whistle-blowing schemes to the fields of accounting, internal accounting controls, auditing matters, fight against bribery, banking and financial crime.

In Portugal, the CNPD has issued the Decision 765/2009, on the principles applicable to whistle-blower hotlines. According to this Decision the whistle-blowing of irregular acts is also restricted to the prevention and/or repression of irregularities such as corruption, banking and financial crime and matters affecting accounts, internal account controls and auditing.

12.2 Is anonymous reporting prohibited, strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do businesses typically address this issue?

Anonymous reporting is not prohibited under EU data protection law; however, it raises problems as regards the essential requirement that personal data should only be collected fairly. In Opinion 1/2006, the WP29 considered that only identified reports should be advertised in order to satisfy this requirement. Businesses should not encourage or advertise the fact that anonymous reports may be made through a whistle-blower scheme.

In its Decision 765/2009, the CNPD repudiates the anonymity. Instead, the controller should adopt a confidentiality regime in order to prevent the risks of slanderous complaints and discrimination.

13 CCTV

13.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?

In Portugal, these notifications took place before the entry into force of the GDPR.

However, a DPIA must be undertaken with assistance from the Data Protection Officer when there is systematic monitoring of a publicly accessible area on a large scale. If the DPIA suggests that the processing would result in a high risk to the rights and freedoms of individuals prior to any action being taken by the controller, the controller must consult the data protection authority.

If the data protection authority is of the opinion that the CCTV monitoring would infringe the GDPR, it has to provide written advice to the controller within eight weeks of the request of a consultation and can use any of its wider investigative, advisory and corrective powers outlined in the GDPR.

13.2 Are there limits on the purposes for which CCTV data may be used?

Yes: only for the purpose of protection of persons and goods.

14 Employee Monitoring

14.1 What types of employee monitoring are permitted (if any), and in what circumstances?

The CNPD has issued Recommendations on the monitoring of use of phone calls, email and internet access by employees at the workplace, as follows:

a. Phone

The controller (employer) shall define the level of tolerance regarding the use of telephones and the forms of control adopted. In cases where monitoring of phone calls takes
place, data other than that which is strictly necessary to achieve the purpose of the control shall not be processed. Undue access to communications, the use of any tapping device, storage, interception and surveillance of the communications by the controller is forbidden.

b. **Email and internet**
The controller shall set up clear and precise rules on the use of the email and internet for private purposes. These rules shall be submitted to the opinion of the data subjects (employees) and their representatives, being expressly publicised. It is advisable that the controller allows the data subjects to use, in moderate and reasonable terms, the new technological means made available to them.

c. **Principles for the use of email**
Even when controllers prohibit the use of emails for private purposes, they are not entitled to open the emails addressed to the data subjects. Non-intrusive control methods must be previously defined and disclosed to the data subjects. The control shall be punctual and towards the areas or activities that present a greater “risk” for the business.

d. **Principles on internet access**
Permanent and systematic control of internet access shall not be undertaken. It shall be done in a global way, not individualised, in relation to all access inside the corporation, with reference to the time of the web connection.

14.2 **Is consent or notice required? Describe how employers typically obtain consent or provide notice.**

There are situations where a data subject will not have a real choice because of an imbalance of power in their relationship with the controller (e.g., between an employer and employee). As such, employers should (by default) avoid reliance on consent as a lawful basis for processing; for instance, (i) execution of the contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract, or (ii) carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security.

14.3 **To what extent do works councils/trade unions/employee representatives need to be notified or consulted?**

The level of use of phone, email and internet at workplace, for private purposes, the delimitation of the conditions for the data processing and the definition of the forms of monitoring adopted shall be included in an Internal Regulation, which shall be submitted to the works councils and publicised (namely, by posting it in the headquarters and in all other workplaces, in order to allow the employees to obtain full knowledge of it).

15 **Data Security and Data Breach**

15.1 **Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?**

Yes. Personal data must be processed in a way which ensures security and safeguards against unauthorised or unlawful processing, accidental loss, destruction and damage of the data.

Depending on the security risk this may include the encryption of personal data, the ability to ensure the ongoing confidentiality, integrity and resilience of processing systems, an ability to restore access to data following a technical or physical incident and a process for regularly testing and evaluating the technical and organisational measures for ensuring the security of processing.

15.2 **Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.**

The controller is responsible for reporting a personal data breach, without undue delay (and in any case within 72 hours of first becoming aware of the breach), to the relevant data protection authority, unless the breach is unlikely to result in a risk to the rights and freedoms of the data subject(s). A processor must notify any data breach to the controller without undue delay.

The notification must include the nature of the personal data breach, including the categories and number of data subjects concerned, the name and contact details of the Data Protection Officer or relevant point of contact, the likely consequences of the breach and the measures taken to address the breach, including attempts to mitigate possible adverse effects.

In Portugal, an official notification form has been approved by the CNPD and can be filed directly online.

15.3 **Is there a legal requirement to report data breaches to affected data subjects? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.**

Controllers have a legal requirement to communicate the breach to the data subject, without undue delay, if the breach is likely to result in a high risk to the rights and freedoms of the data subject.

The notification must include the name and contact details of the Data Protection Officer (or point of contact), the likely consequences of the breach and any measures taken to remedy or mitigate the breach.

The controller may be exempt from notifying the data subject if the risk of harm is remote (e.g., because the affected data is encrypted), the controller has taken measures to minimise the risk of harm (e.g., suspending affected accounts) or the notification requires a disproportionate effort (e.g., a public notice of the breach).

15.4 **What are the maximum penalties for data security breaches?**

The maximum penalty is the higher of €20 million or 4% of worldwide turnover.
16.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?

Yes. No court order is required.

16.3 Describe the data protection authority’s approach to exercising those powers, with examples of recent cases.

On October 2018, the CNPD fined Barreiro-Montijo Hospital Centre (“Hospital”) in the amount of €400,000, based on its policies regarding access to databases, which allowed technicians and physicians to consult patients’ clinical files without proper authorisation. This action was based on the fact that professionals working in the area of social services had access to patients’ personal data files which should have been exclusively reserved to physicians. The CNPD concluded that the Hospital had no internal rules for the creation of accounts or for granting different levels of access to clinical information.

The following (three) infractions were identified: violation of the principle of data integrity and confidentiality; violation of the principle of data minimisation which should prevent indiscriminate access to clinical data of patients; and the inability of the Hospital, as controller, to ensure the confidentiality and integrity of the data. The first two infringements were punished with a fine of €150,000 each, with a further €100,000 fine handed down for the third.

16.4 Does the data protection authority ever exercise its powers against businesses established in other jurisdictions? If so, how is this enforced?

We are not aware of any such cases.

17 E-discovery / Disclosure to Foreign Law Enforcement Agencies

17.1 How do businesses typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?

Portuguese businesses typically respond that they are subject to EU personal data protection obligations, namely those regarding confidentiality and the impossibility to share data without legitimate grounds. In Portugal, there is a conflict between the data protection law and e-discovery demands, which is strengthened by the differences between the different judicial systems. In these cases, the reply to foreign e-discovery requests is always limited by compliance with Portuguese and EU legislation on data protection.

17.2 What guidance has/have the data protection authority(ies) issued?

Although the CNPD has not provided any specific guidelines on this issue, the implications of e-discovery exercises are relatively easy to identify:

a. Furnishing adequate notice to affected Portuguese individuals.

b. Ensuring the underlying legitimacy of the collection and processing (and, frequently, international transfer) of personal data.

c. Maintaining appropriate limitations or controls on the scope of the data collection exercises.

d. Abiding by international data transfer rules.
18 Trends and Developments

18.1 What enforcement trends have emerged during the previous 12 months? Describe any relevant case law.

Portuguese courts have been deciding that the images captured by CCTV are admissible as proof in a disciplinary proceeding and in the subsequent legal action, provided that the requirements arising from the legislation on data protection have been met, and that the purpose of their placement was not solely to control workers’ professional performance.

According to the Portuguese legislation, the employer may not use remote monitoring equipment in the workplace for controlling the worker’s professional performance. However, the use of this equipment is acceptable whenever it has as its purpose the protection and security of people and goods, or when particular requirements inherent to the nature of the activity justify such use.

The most relevant decision in this matter is a ruling from the Court of Appeal of Oporto, of October 2018, that considered as a legitimate proof for disciplinary means the visualisation of CCTV images that were collected at the workplace. Since CCTV has been duly authorised by the CNPD for protecting people and goods, and the worker had knowledge that her workplace was under video surveillance, the Court ruled that it is permissible to view, in a court hearing, images from video surveillance collected at the workplace as proof for disciplinary purposes.

18.2 What “hot topics” are currently a focus for the data protection regulator?

The following topics are being looked at closely:

a. The implementation of the new national data protection law that will complement the GDPR in Portugal.

b. The protection of students’ personal data online (viz. the publication of evaluations).

c. The implementation and enforcement of the GDPR – the CNPD has published several documents to guide controllers and processors in this process.
Having joined Cuatrecasas in 2008, Sónia Queiróz Vaz is now a Senior Associate coordinating the firm’s Intellectual Property, Media and Data Protection department in Portugal.

Sónia has advised on projects involving the evaluation and verification of compliance with obligations relating to personal data and privacy protection, has helped map how personally identifiable information is processed, and has defined strategies for implementing the requirements of the General Data Protection Regulation.

She is experienced in drafting and negotiating agreements for the exploitation of intellectual property rights (particularly, licensing and transfer rights) in many fields (including broadcasting, publishing and merchandising). She has extensive expertise in the commercial exploitation of software and audiovisual products domestically and internationally.

Sónia has also provided legal advice on projects concerning consumer rights, industrial property rights, advertising rights and social communication rights.

She has been a member of the Portuguese Bar since 2000.

Education:
- Course on IP and Competition Law, Católica Global School of Law, 2016.
- Law Degree from the University of Lisbon Law School, 2000.

Ana Costa Teixeira has been an Associate Lawyer at Cuatrecasas since 2008.

Ana focuses her practice on the areas of intellectual property, advertising and media law, new technologies law (computer law) and data protection law, providing advice, in particular, on conflicts relating to intellectual and industrial property rights, unfair competition and advertising, and distribution and licence agreements.

Previously, she worked at Almeida Sampaio & Associados.

She has been a member of the Portuguese Bar Association since 2002.

Ana has also been a teacher at IADE, on the subject of Legal Protection of Trademarks and Branding and Trademark Management (Postgraduate Course), since 2011.

Education:
- Law Degree, University of Lisbon Law School, 2002.
- Postgraduate Course in Administrative Litigation, School of Law of the Catholic University, 2006.
- Summer Course on Industrial Property, University of Lisbon Law School, 2008.
Chapter 38

Senegal

LPS L@w

Léon Patrice Sarr

1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?


The DPA and its application decree provide the conditions relating to data processing, the rights of Data Subjects and the obligations of Data Controllers. The DPA creates the Senegalese Data Protection Authority (Commission de Protection des Données Personnelles) (CDP) Law no. 2016-29 dated 8 November 2016 modifying the penal code, which provides criminal offences relating to data processing and the applicable sanctions.

1.2 Is there any other general legislation that impacts data protection?

There is no other general legislation that impacts data protection.

1.3 Is there any sector-specific legislation that impacts data protection?

There is no sector-specific legislation that impacts data protection.

1.4 What authority(ies) are responsible for data protection?

The authority responsible for data protection is the Senegalese Data Protection Authority (Commission de Protection des Données Personnelles) (CDP).

2 Definitions

2.1 Please provide the key definitions used in the relevant legislation:

- **“Personal Data”**
  
  “Personal Data” means all data relating to an identified or identifiable individual with reference to an identification number or one, or many, characteristics of his physical, physiological, genetic, psychical, cultural, social and economic identity.

- **“Processing”**
  
  “Processing” of personal data (or “Data Processing”) means any operation or set of operations in relation to such data, especially their collection, exploitation, registration, organisation, storage, adaptation, modification, retrieval, backup, copying, consultation, utilisation, disclosure by transmission, dissemination or otherwise making available, alignment, locking, encryption, erasure or destruction.

- **“Controller”**
  
  “Controller” means all persons who (either alone, or jointly or in common with other persons) takes the decision to collect and process personal data and determines the purposes of the processing.

- **“Processor”**
  
  “Processor” means all persons who (either alone, or jointly or in common with other persons) collect, exploit, register, organise, store, adapt, modify, retrieve, backup, copy, consult, use or disclose data by transmission, dissemination or otherwise making available, alignment, locking, encryption, erasure or destruction.

- **“Data Subject”**
  
  “Data Subject” means all individual persons whose personal data are processed.

- **“Sensitive Personal Data”**
  
  “Sensitive Personal Data” means data relating to: religious, philosophical or political opinions or union activities; sex life; race; health; social measures and prosecutions; and criminal and administrative sanctions.

- **“Data Breach”**
  
  “Data Breach” means any operation or attempted operation involving such data, especially its interception, misappropriation, damage, deletion, erasure, alteration or counterfeiting by an unauthorised production, use, backup or transfer process.

Other key definitions – please specify (e.g., “Pseudonymous Data”, “Direct Personal Data”, “Indirect Personal Data”)

There are no other specific key definitions.
### 3 Territorial Scope

3.1 Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to those laws?

Yes, if the business’s means of processing are located in Senegal, unless they are for transit only.

### 4 Key Principles

#### 4.1 What are the key principles that apply to the processing of personal data?

- **Transparency**
  
  Under Article 35 of the DPA, Data Controllers must inform the Data Subjects about the processing and personal data processed.

- **Lawful basis for processing**
  
  Under Article 34 of the DPA, personal data must be processed lawfully and fairly.

- **Purpose limitation**
  
  Under Article 35 of the DPA, personal data may only be obtained for specific, explicit and legitimate purposes, and cannot be further processed in any manner incompatible with those purposes.

- **Data minimisation**
  
  Under Article 35 of the DPA, personal data must be adequate, relevant and not excessive in relation to the purposes for which they are collected and further processed.

- **Proportionality**
  
  Refer to “Data minimisation”.

- **Retention**
  
  Under Article 35 of the DPA, personal data must not be retained for longer than is necessary for the purposes for which they are collected and further processed.

- **Other key principles – please specify**

  - **Confidentiality**
    
    Under Article 35 of the DPA, the Data Controller must ensure confidentiality and security of the processing.

  - **Legitimacy**
    
    Under Article 33 of the DPA, the processing of personal data is legitimate if the Data Subject consents to the processing. The consent must be express, unequivocal, free and specific.

    However, under Article 33 of the DPA, processing can be justified without the Data Subject’s consent on any of the following grounds: compliance with any legal obligation to which the Data Controller is subject; performance of a public service undertaking that has been entrusted to the Data Controller or the data recipient; the processing relates to the performance of a contract to which the Data Subject is a party, or of pre-contractual measures requested by him; and processing the data is subject to the interests and fundamental rights and liberties of the Data Subject.

### 5 Individual Rights

#### 5.1 What are the key rights that individuals have in relation to the processing of their personal data?

- **Right of access to data/copies of data**
  
  Pursuant to Article 62 of the DPA, Data Subjects have a right of access and they can obtain the following from the Data Controller:
  
  - Information which they are entitled to know and which will allow them to contest the processing.
  - Confirmation of whether their personal data forms part of the processing.
  - A copy of their personal data (in an accessible form), as well as any available information on the data’s origin.
  - Information relating to the: purposes of the processing; categories of processed data; recipients or categories of recipients to whom the data are disclosed; and transfer of personal data outside the country.

    The right of access is limited when the processing involves state security, defence or public safety.

- **Right to rectification of errors**
  
  Pursuant to Article 69 of the DPA, Data Subjects can request that the Data Controller rectifies or deletes their personal data if they are inaccurate, incomplete, unclear or expired, or if the collection, usage, disclosure or retention of the data is prohibited.

- **Right to deletion/right to be forgotten**
  
  Relating to the right to deletion, refer to “Right to rectification of errors”. There is no “right to be forgotten” in current Senegalese law.

- **Right to object to processing**
  
  Pursuant to Article 63 of the DPA, Data Subjects have the right to object to the processing on legitimate grounds, unless the processing satisfies a legal obligation.

- **Right to restrict processing**
  
  Refer to “Right to object to processing”.

- **Right to data portability**
  
  There is no such right in Senegalese law.

- **Right to withdraw consent**
  
  Pursuant to Article 33 of the DPA, data processing requires the Data Subject’s prior consent. However, his consent is not required in the following instances:
  
  - If required by the law.
  - To fulfil a general interest mission or required by the public authority.
  - For an agreement execution if the processor is party to the contract.
  - For fundamental freedoms and personal interest safeguarding.

- **Right to object to marketing**
  
  Data Subjects have the right to object, free of charge, to the processing of their Personal Data for direct marketing.

- **Right to complain to the relevant data protection authority(ies)**
  
  Data Subjects can complain to the CDP at any time the processing of their Personal Data does not comply with the DPA provisions.

  - **Other key rights – please specify**
    
    There are no other specific key rights.
### 6 Registration Formalities and Prior Approval

#### 6.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?

Under Article 18 of the DPA, businesses must notify the CDP in respect of their processing activities, except in the following cases:

- Non-profit processing for religious, philosophical or political associations, or trade unions (when the data correspond to the purpose of the association or trade union, concern only their members and are not disclosed to third parties).
- Processing for the sole purpose of keeping a register; by law, this is intended exclusively to provide public information and is open to consultation for any person with a legitimate interest.

#### 6.2 If such registration/notice is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?

The notification/registration must be specific.

#### 6.3 On what basis are registrations/notifications made (e.g., per legal entity, per processing purpose, per data category, per system or database)?

Notifications are made per processing purpose.

#### 6.4 Who must register with/notify the data protection authority (e.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation)?

Pursuant to Article 22 of the DPA, the Data Controller must notify the data protection authority regardless of whether he is a local or foreign legal entity. If the Data Controller is not established in Senegal, he must communicate to the data protection authority his legal representative in Senegal.

#### 6.5 What information must be included in the registration/notification (e.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes)?

The declaration must include the following:

- Identity and address of the Data Controller or his representative.
- Purpose(s) of the processing and the description of its general functions.
- Possible interconnections between databases.
- Personal data processed and categories of persons concerned in its processing.
- Time period for which the data will be kept.
- Department or person(s) in charge of data processing.
- Recipient(s) or categories of recipients of the processed data.
- Persons or departments before which the right of access is exercised.
- Measures taken to ensure the security of the processing.
- Identity and address of the data processor.

#### 6.6 What are the sanctions for failure to register/notify where required?

Sanctions for failure to register/notify are:

- Imprisonment for a period of between one and seven years.
- Fines of between XOF 500,000 and 10 million.

The judge can choose one of the sanctions listed above or a combination of them.

#### 6.7 What is the fee per registration/notification (if applicable)?

There is no fee.

#### 6.8 How frequently must registrations/notifications be renewed (if applicable)?

Notifications must be renewed any time the information provided changes.

#### 6.9 Is any prior approval required from the data protection regulator?

Under Article 20 of the DPA, prior approval from the CDP is required for processing of:

- Genetic data.
- Data relating to offences, convictions or security measures.
- Data that involve an interconnection of files.
- Data that include a national identification number.
- Biometric data.
- Data that are of public interest, particularly for historical, statistical or scientific purposes.

Authorisation is not required in the following cases:

- Data processing for private purposes only.
- Temporary data copies for transmission, network access and automatic storage purposes, as long as it is made to improve network user access.
- Data processing by non-profit organisations for religious, political or union purposes only.
- Data processing for public register purposes.

#### 6.10 Can the registration/notification be completed online?

Notifications cannot be completed online but they can be sent online.

#### 6.11 Is there a publicly available list of completed registrations/notifications?

The list of completed notifications is available on the Senegalese Data Protection Authority website: [http://www.cdp.sn/repertoire-des-declarations](http://www.cdp.sn/repertoire-des-declarations).
6.12 How long does a typical registration/notification process take?

A typical notification process takes one month, unless extended (once) by a motivated decision from the CDP.

7 Appointment of a Data Protection Officer

7.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.

There is no provision relating to the appointment of a Data Protection Officer. However, the DPA provides that the person or department where the access right is exercised must be communicated to the CDP.

7.2 What are the sanctions for failing to appoint a Data Protection Officer where required?

There are no sanctions.

7.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect of his or her role as a Data Protection Officer?

There is no particular protection for Data Protection Officers.

7.4 Can a business appoint a single Data Protection Officer to cover multiple entities?

There are no legal limitations.

7.5 Please describe any specific qualifications for the Data Protection Officer required by law.

There are no specific qualifications required by law.

7.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?

There is no provision on the responsibilities of Data Protection Officers in the DPA.

7.7 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?

The DPA does not provide that the Data Protection Officer must be notified to the CDP. However, under Article 22 of the DPA, the person or department where the access right is exercised must be communicated to the CDP.

7.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?

The DPA does not provide that Data Protection Officers must be named in a public-facing privacy notice or equivalent document.

8 Appointment of Processors

8.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?

The business shall sign a subcontract agreement with the processor.

8.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?

Under the provisions of Article 39 of the DPA, the subcontract agreement must be written and must stipulate that the subcontractor must only process personal data in accordance with the processor’s instructions. He must also take every necessary measure to ensure the data’s security and safety.

9 Marketing

9.1 Please describe any legislative restrictions on the sending of electronic direct marketing (e.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?).

The sending of marketing communications is forbidden pursuant to Article 47 of the DPA and Article 16 of the Senegalese Electronic Transactions Law unless the recipient agrees to it. However, there are two exceptions where prior approval is not required:

- The recipient’s information was collected directly from him, in accordance with the provisions of the DPA.
- The recipient is already a customer of the company, the marketing messages relate to products or services that are similar to those previously provided, and the recipient is given the possibility to object to all messages sent to him.

9.2 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.).

Article 47 of the DPA does not distinguish the means used.

9.3 Do the restrictions noted above apply to marketing sent from other jurisdictions?

Yes, the restrictions above apply to marketing sent from other jurisdictions.

9.4 Is/are the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?

Yes. Since 2014, the CDP has sent several warnings and notices to different companies for breaches of marketing restrictions. For example:

- EXPRESSO TELECOM was sent a warning on 3 April 2014 for unrequested advertisement.
9.5 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?

Pursuant to Article 47 of the DPA, it is unlawful to purchase marketing lists from third parties.

9.6 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?

According to Article 431-20 of the Senegalese Criminal Law, the maximum penalties for sending marketing communications in breach of applicable restrictions are seven years' imprisonment and a XOF 1 million fine, or only one of these sentences.

10 Cookies

10.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).

There is no provision relating to the use of cookies.

10.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?

This is not applicable in Senegal.

10.3 To date, has/have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?

This is not applicable in Senegal.

10.4 What are the maximum penalties for breaches of applicable cookie restrictions?

This is not applicable in Senegal.

11 Restrictions on International Data Transfers

11.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.

Pursuant to Article 49 of the DPA, transfer of personal data to another country is prohibited unless the receiving country provides sufficient protection for the Data Subject’s private life, liberties and fundamental rights.

11.2 Please describe the mechanisms businesses typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).

The transfer of personal data abroad is possible only if the recipient country offers a sufficient level of protection of privacy, liberty and fundamental rights to Data Subjects. Before transferring personal data, the company must inform the CDP. The information must include:

- The name and address of the data sender.
- The name and address of the data recipient.
- The full data file and description.
- The type of personal data transferred.
- The number of concerned persons.
- The data processing purpose.
- The transfer method and frequency.
- The first transfer date.

A transfer to a country not offering a sufficient level of protection is possible if the transfer is timely and non-massive, if the Data Subject agrees to it or if the transfer is necessary to:

- protect the life of the Data Subject;
- protect the public interest;
- comply with obligations allowing the acknowledgment, exercise or defence of a legal right in court; and
- perform an agreement between the Data Subject and the Data Processor or take precontractual measures upon the request of the Data Subject.

The CDP can allow a transfer to a country that does not offer a sufficient level of protection, based on reasoned request, if the Data Processor offers sufficient guarantees of privacy, liberty and fundamental rights to Data Subjects.

11.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.

The transfer of personal data to a country that provides sufficient protection requires notification to the CDP before the transfer. The Data Controller fills in and files the notification form. All changes in the information notified must be declared to the CDP within 15 working days. The CDP was supposed to establish a list of the countries that offer sufficient protection. However, so far, the list does not exist.

The transfer of personal data to a country that does not provide sufficient protection requires prior authorisation from the CDP. The Data Controller must fill in and file the authorisation request form. The CDP issues the decision within two months, extendable once. The Data Controller must file another authorisation request if any change affects the information provided to the CDP.
12 Whistle-blower Hotlines

12.1 What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?

To the best of our knowledge, there is no legal provision or binding guidance issued by the CDP on corporate whistle-blower hotlines.

12.2 Is anonymous reporting prohibited, strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do businesses typically address this issue?

This is not applicable in Senegal.

13 CCTV

13.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?

The CDP issued deliberation no. 2015-00186/CDP dated 8 January 2016 relating to CCTV surveillance, and deliberation no. 2016-00238 dated 11 November 2016 relating to the rules governing CCTV installation and exploitation in workplaces, which state that the use of CCTV requires a separate notification to the CDP. However, data collected and stored abroad require prior authorisation from the CDP.

13.2 Are there limits on the purposes for which CCTV data may be used?

A CCTV system may be used only:

- For assets and self-security purposes when used by individuals. In such case, the CCTV system must only cover the house perimeter.
- For security and infringement prevention or recognition in public areas – the reasons for which it is used by public authorities.
- For business premises’ security and access, or the monitoring of employees’ movements, when used by private corporations.

Any other use requires CDP approval.

14 Employee Monitoring

14.1 What types of employee monitoring are permitted (if any), and in what circumstances?

Pursuant to deliberation no. 2016-00238, employee monitoring is allowed for employee and asset security. A CCTV system cannot be used for employee monitoring only.

A CCTV system can be installed in the following places:

- Premises’ entrances and exits.
- Corridors and hallways.
- Emergency exits.

15 Data Security and Data Breach

15.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?

Pursuant to Article 71 of the DPA, Data Controllers are required to ensure the security of personal data. They must prevent the data’s alteration and damage, or access by non-authorised third parties. Additionally, Data Controllers must make sure that:

- Persons with access to the system can only access the data that they are allowed to.
- The identity and interest of any third-party recipients of the data can be verified.
- The identity of persons who have access to the system (to view the data or add data) can be verified.
- Unauthorised persons cannot access the place and equipment used for the data processing.
- Unauthorised persons cannot read, copy, modify, destroy or move data.
- All data introduced in the system are authorised.
- The data will not be read, copied, modified or deleted without authorisation during the transport or communication of the data.
The data are backed up with security copies.
The data are renewed and converted in order to preserve them.

15.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expects voluntary breach reporting.

There is no legal requirement to report data breaches to the CDP.

15.3 Is there a legal requirement to report data breaches to affected data subjects? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expects voluntary breach reporting.

There is no legal requirement to report data breaches to individuals.

15.4 What are the maximum penalties for data security breaches?

The maximum criminal penalty for security breaches is imprisonment for one to seven years and a fine of between XOF 500,000 and XOF 10 million, or one of these penalties. In addition, the CDP can impose an administrative fine of between XOF 1 million and XOF 100 million.

16 Enforcement and Sanctions

16.1 Describe the enforcement powers of the data protection authority(ies).

<table>
<thead>
<tr>
<th>Investigatory Power</th>
<th>Civil/Administrative Sanction</th>
<th>Criminal Sanction</th>
</tr>
</thead>
<tbody>
<tr>
<td>The CDP can conduct three types of investigation:</td>
<td>The CDP can impose the following:</td>
<td>Criminal sanctions are pronounced by Courts. They are:</td>
</tr>
<tr>
<td>■ On-site inspections</td>
<td>■ following sanctions in cases of breach of the DPA:</td>
<td>■ imprisonment for a period of between six months and seven years; and</td>
</tr>
<tr>
<td>In this case, the CDP may have access to any materials (servers, computers, applications, etc.) and any place (offices, buildings) in which personal data are processed.</td>
<td>■ provisional withdrawal for three months of the given authorisation; the withdrawal becomes definitive at the end of the three-month period if the breach remains; and</td>
<td>■ fines of between XOF 200,000 and XOF 10 million.</td>
</tr>
<tr>
<td>■ Documentary inspections</td>
<td>■ fines of between XOF 1 million and XOF 100 million.</td>
<td>In cases of urgency, the CDP can also:</td>
</tr>
<tr>
<td>These inspections allow the CDP to obtain disclosure of documents or files upon written request.</td>
<td>In cases of urgency, the CDP can also:</td>
<td>■ interrupt the processing for a duration which cannot exceed three months;</td>
</tr>
</tbody>
</table>

16.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?

Pursuant to Article 31 of the DPA, the CDP has the power to issue a temporary or a permanent ban. The ban does not require a court order.

16.3 Describe the data protection authority’s approach to exercising those powers, with examples of recent cases.

After its installation in December 2013, the CDP published a press release inviting Data Controllers to notify it of the processing of their data. The CDP also sent letters directly to certain companies for the same purpose. The companies who failed to notify or to provide the additional information requested by the CDP received either a notice or a warning. The CDP also sent several notices and warnings to different companies for breach of the restrictions on the sending of marketing communications. To the best of our knowledge, there has been no fine imposed so far.

On 3 April 2014, EXPRESSO received a warning for failure to notify the processing and failure to respect the restrictions on the sending of marketing communications.

On 30 April 2014, SONATEL received a notice for failure to notify the database relating to the sending of marketing communications, failure to respect the restrictions on the sending of marketing communications, and failure on security and confidentiality measures.

On 30 April 2014, TIGO received a notice for failure to notify its processing and failure to respect the restrictions on the sending of marketing communications.

On 15 May 2015, DIGITAL VIRGO received a warning for failure to request the consent of Data Subjects and their rights of information and objection, and failure to respect the restrictions on the sending of marketing communications.

On 15 May 2015, DIGITAL VIRGO received a warning for failure to request the consent of Data Subjects and their rights of information and objection, and failure to respect the restrictions on the sending of marketing communications.

On 31 July 2015, HELLO FOOD SENEGAL received a warning for failure to notify the processing of personal data, failure to respect the fundamental principles of data protection, failure to respect the rights of Data Subjects, and failure to respect the restrictions on the sending of marketing communications.

On 6 November 2015, AFRIQUE PETROLE received a warning for monitoring employees’ private emails.
16.4 Does the data protection authority ever exercise its powers against businesses established in other jurisdictions? If so, how is this enforced?

The CDP does not exercise its powers against businesses established in other jurisdictions.

17 E-discovery / Disclosure to Foreign Law Enforcement Agencies

17.1 How do businesses typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?

We have no information on how businesses respond to foreign e-discovery requests or requests for disclosure from foreign law enforcement agencies. This information is not public.

17.2 What guidance has/have the data protection authority(ies) issued?

The CDP has issued no guidance on this topic.

18 Trends and Developments

18.1 What enforcement trends have emerged during the previous 12 months? Describe any relevant case law.

There has been no emergence of any enforcement trends during the previous 12 months. The CDP has so far opted to send notices and warnings because Data Controllers generally react positively by complying with the DPA provisions.

18.2 What “hot topics” are currently a focus for the data protection regulator?

The CDP current “hot topic” is the creation in Senegalese law of a right to be forgotten. The CDP authorities agree and admit that every Senegalese citizen should have the right to obtain the withdrawal of published compromising or personal information. Unfortunately, as yet, no legal measure has been taken to this end.
1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

The Personal Data Protection Act 2012 (No. 26 of 2012) ("PDPA") is the principal data protection legislation in Singapore. The PDPA establishes a general data protection law which applies to all private sector organisations.

Parts III to VI of the PDPA set out obligations of organisations in respect of the collection, use, disclosure, access, correction, care, protection, retention, and transfer of personal data (collectively, "Data Protection Provisions"); while Part IX of the PDPA sets out provisions pertaining to Singapore’s national Do Not Call ("DNC") Registry and the obligations of organisations in relation to sending marketing messages to Singapore telephone numbers ("DNC Provisions").

Other regulations issued under the PDPA are:
- the Personal Data Protection Regulations 2014 ("PDP Regulations"), which sets out the requirements for transfers of personal data out of Singapore; the form, manner and procedures for requests for access to or correction of personal data; and persons who may exercise rights in relation to disclosure of personal data of deceased individuals;
- the Personal Data Protection (Composition of Offences) Regulations 2013;
- the Personal Data Protection (Do Not Call Registry) Regulations 2013;
- the Personal Data Protection (Enforcement) Regulations 2014; and
- the Personal Data Protection (Appeal) Regulations 2015.

In addition, the Personal Data Protection Commission ("PDPC") has issued a number of advisory guidelines which provide greater clarity on the interpretation of the PDPA.

1.2 Is there any other general legislation that impacts data protection?

The Computer Misuse Act (Cap. 50A) sets out a number of offences which include the unauthorised access or modification of computer material, as well as the unauthorised use or interception of computer services.

The Cybersecurity Act (No. 9 of 2018) requires owners and operators of Critical Information Infrastructure to comply with cybersecurity policies and standards, conduct audits and risk assessments, and implement incident reporting measures.

For completeness, the Spam Control Act (Cap. 311A) ("SCA") regulates the bulk sending of unsolicited commercial electronic messages to email addresses or mobile telephone numbers, complementing the DNC Provisions of the PDPA. The DNC Provisions of the PDPA and the SCA are expected to be merged into a new Act dealing with unsolicited commercial electronic messages generally.

1.3 Is there any sector-specific legislation that impacts data protection?

Yes, a number of other legislation and regulatory requirements in Singapore contain certain sector-specific data protection requirements. For example:
- the Banking Act (Cap. 19) ("Banking Act") contains a number of banking secrecy provisions which govern customer information obtained by banks;
- the Telecoms Competition Code issued under the Telecommunications Act (Cap. 323) governs the use of end-user service information by telecoms licensees; and
- the Private Hospitals and Medical Clinics Act (Cap. 248) and the licensing terms and conditions issued thereunder contain provisions addressing the confidentiality of medical information and the retention of medical records.

With regards to the financial sector, the Monetary Authority of Singapore ("MAS") is empowered under the Monetary Authority of Singapore Act (Cap. 186) and other sectoral legislation to issue directives and notices. Examples of MAS-issued regulatory instruments which are relevant to data protection include the Notices and Guidelines on Technology Risk Management, and the Guidelines on Outsourcing.

In this regard, Section 4(6) of the PDPA provides that the general data protection framework does not affect any right or obligation under the law, and that in the event of any inconsistency, the provisions of other written laws will prevail.

The PDPC has also developed sector-specific advisory guidelines for the telecommunication sector, the real estate agency sector, the education sector, the healthcare sector, the social service sector and transport services for hire (specifically in relation to in-vehicle recordings).

In addition, the PDPC has also provided comments and suggestions to industry-led guidelines on the PDPA that were developed by industry associations such as:
1.4 What authority(ies) are responsible for data protection?

The PDPC is responsible for administering and enforcing the PDPA. The PDPC is a statutory body under the purview of the Ministry of Communications and Information (“MCI”), and is part of the merged info-communications and media regulator, the Info-communications Media Development Authority of Singapore (“IMDA”) (previously the Info-communications Development Authority of Singapore and the Media Development Authority of Singapore).

Sector-specific data protection obligations are separately enforced by the relevant sectoral regulators. For example, the MAS enforces the banking secrecy provisions under the Banking Act and the relevant provisions under other sectoral legislation and regulatory instruments governing other types of financial institutions.

2 Definitions

2.1 Please provide the key definitions used in the relevant legislation:

- **“Personal Data”**
  “Personal data” is defined under the PDPA as data, whether true or not, about an individual who can be identified: (a) from that data; or (b) from that data and other information to which the organisation is likely to have access.

  All formats of personal data are covered under the PDPA, whether electronic or non-electronic, and regardless of the degree of sensitivity.

- **“Processing”**
  Under the PDPA, “processing”, in relation to personal data, means the carrying out of any operation or set of operations in relation to the personal data, and includes any of the following:
  - (a) recording;
  - (b) holding;
  - (c) organisation, adaptation or alteration;
  - (d) retrieval;
  - (e) combination;
  - (f) transmission; and
  - (g) erasure or destruction.

- **“Controller”**
  The PDPA does not refer to the concept of a “controller”, and instead refers to an “organisation”. An “organisation” is defined as any individual, company, association or body of persons, corporate or unincorporated, whether or not: (a) formed or recognised under the law of Singapore; or (b) resident, or having an office or a place of business, in Singapore.

- **“Processor”**
  Similarly, the PDPA does not use the term “processor”, and instead refers to a “data intermediary”, which is defined as an organisation which processes personal data on behalf of another organisation but does not include an employee of that other organisation.

The PDPA provides that a data intermediary that processes personal data on behalf of and for the purposes of another organisation pursuant to a contract which is evidenced or made in writing will only be subject to the Protection Obligation and the Retention Limitation Obligation (as defined below).

- **“Data Subject”**
  The PDPA does not refer to the concept of a “data subject”, and instead refers generally to an “individual”, whose personal data is collected, used, disclosed, or otherwise processed by organisations. An “individual” is defined to mean a natural person, whether living or deceased.

- **“Sensitive Personal Data”**
  The PDPA does not distinguish between specific categories of personal data. The term “sensitive personal data” is therefore not defined.

However, as a number of the Data Protection Provisions adopt a standard of reasonableness, the sensitivity of the personal data in question could, in practice, affect the extent of the data protection obligations an organisation is subject to. The PDPC has taken the position in several enforcement decisions that a higher standard of protection is required for more sensitive personal data, which includes insurance, medical and financial data (see in Re Aviva Ltd [2017] SGPDPC 14).

In this regard, the PDPC’s Advisory Guidelines on Enforcement for Data Protection Provisions (“Enforcement Guidelines”) provides that, if an organisation who has breached a Data Protection Obligation is in the business of handling large volumes of sensitive personal data, the disclosure of which may cause exceptional damage, injury, or hardship to a person (such as medical or financial data), but failed to put in place adequate safeguards proportional to the harm that might be caused by disclosure of such personal data, the PDPC may consider this to be an aggravating factor in calculating the level of the financial penalty to be imposed on the organisation.

- **“Data Breach”**
  The PDPA does not define “data breach”. However, the PDPC, in its Guide to Managing Data Breaches, refers to a “data breach” as the “unauthorised access and retrieval of information that may include corporate and personal data”. An organisation is required under Section 24 of the PDPA to protect personal data against the unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks.

**Other key definitions – please specify (e.g. “Pseudonymous Data”, “Direct Personal Data”, “Indirect Personal Data”)**

There are no other applicable key definitions.

3 Territorial Scope

3.1 Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to those laws?

The PDPA applies to all organisations which are not a public agency or acting on behalf of a public agency, whether or not formed or recognised under the laws of Singapore, or resident or having an office or a place of business in Singapore.

According to the PDPC’s Advisory Guidelines on Key Concepts in the PDPA (“Key Concepts Guidelines”), the Data Protection Provisions apply to organisations carrying out activities involving personal data in Singapore. Thus, where personal data is collected overseas and subsequently transferred into Singapore, the Data Protection Provisions will apply in respect of the activities involving the personal data in Singapore.
4 Key Principles

4.1 What are the key principles that apply to the processing of personal data?

- **Transparency**
  Section 20 of the PDPA provides that an organisation must notify an individual of the purpose(s) for which it intends to collect, use, or disclose his personal data, on or before such collection, use, or disclosure (Notification Obligation). More generally, Section 12 of the PDPA requires an organisation to develop and implement policies and practices that are necessary for the organisation to meet its obligations under the PDPA, and make information about its policies and procedures publicly available (Openness Obligation).

- **Lawful basis for processing**
  Sections 13 to 17 of the PDPA generally require that an organisation obtain the consent of an individual before collecting, using, or disclosing his personal data for a purpose (Consent Obligation). Unless an exception in the Second, Third or Fourth Schedule to the PDPA applies, such consent from an individual must be validly obtained and may be either expressly given or deemed to have been given.

- **Purpose limitation**
  Section 18 of the PDPA provides that an organisation may collect, use or disclose personal data about an individual only for purposes that a reasonable person would consider appropriate in the circumstances and, if applicable, have been notified to the individual concerned (“Purpose Limitation Obligation”).

- **Data minimisation**
  The PDPA does not articulate the principle of data minimisation (i.e., the limitation of personal data collection to what is directly relevant and necessary to accomplish a specified purpose), although the Purpose Limitation Obligation and Retention Limitation Obligation (as defined below) operate to limit the collection, use, disclosure and retention of personal data by organisations to some extent. As a best practice, the PDPC recommends that organisations avoid the over-collection of personal data, where this is not required for their business or legal purposes. Instead, the PDPC encourages organisations to consider whether there are alternative ways of addressing their requirements.

- **Proportionality**
  While the PDPA does not explicitly refer to the principle of proportionality, a number of the Data Protection Provisions – namely, the Purpose Limitation Obligation, the Accuracy Obligation, the Protection Obligation, and the Retention Limitation Obligation (as defined below) – make reference to a standard of reasonableness. More generally, Section 11(1) of the PDPA states that an organisation shall, in meeting its responsibilities under the PDPA, “consider what a reasonable person would consider appropriate in the circumstances”. In this regard, the PDPC’s Key Concepts Guidelines states that a “reasonable person” is judged based on an objective standard and can be said to be a person who exercises the appropriate care and judgement in the particular circumstances.

- **Retention**
  While the PDPA does not prescribe any specific data retention periods, Section 25 of the PDPA provides that an organisation must cease to retain documents containing personal data, or remove the means by which the personal data can be associated with particular individuals as soon as it is reasonable to assume that (a) the purpose for which the personal data was collected is no longer being served by retention of the personal data, and (b) retention is no longer necessary for legal or business purposes (“Retention Limitation Obligation”).

Other key principles – please specify

- Section 23 of the PDPA requires an organisation to make a reasonable effort to ensure that personal data collected by or on behalf of the organisation is accurate and complete, if the personal data is likely to be used by the organisation to make a decision that affects the individual to whom the personal relates, or is likely to be disclosed by the organisation to another organisation (“Accuracy Obligation”).

- Section 24 of the PDPA requires an organisation to make reasonable security arrangements to protect personal data in its possession or under its control, in order to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks (“Protection Obligation”) (see our response to section 15 below).

- Section 26 of the PDPA provides that an organisation must not transfer any personal data to a country or territory outside Singapore, except in accordance with prescribed requirements to ensure that organisations provide a standard of protection to the transferred personal data that is comparable to the protection under the PDPA (“Transfer Limitation Obligation”) (see our response to section 11 below).

5 Individual Rights

5.1 What are the key rights that individuals have in relation to the processing of their personal data?

- **Right of access to data/copies of data**
  Under Section 21 of the PDPA, an individual has the right to request an organisation to allow him access to his personal data. Specifically, unless a relevant exception under the PDPA applies, an organisation is required to, on request by an individual, provide him with: (a) his personal data in the possession or under the control of the organisation; and (b) information about the ways in which that personal data has been or may have been used or disclosed by the organisation within a year before the date of the individual’s request (“Access Obligation”).

  There are a number of exceptions to the Access Obligation. Specifically, an organisation is not required to provide an individual with his personal data or other information, in respect of the matters specified under the Fifth Schedule to the PDPA, which include, without limitation:

  - opinion data kept solely for an evaluative purpose;
  - personal data which, if disclosed, would reveal confidential commercial information that could, in the opinion of a reasonable person, harm the competitive position of the organisation;
  - personal data collected, used or disclosed without consent, for the purposes of an investigation if the investigation and associated proceedings and appeals have not been completed; and

  any request:

  - that would unreasonably interfere with the operations of the organisation because of the repetitious or systematic nature of the requests;
6 Registration Formalities and Prior Approval

6.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?

There is currently no requirement for organisations to register with or notify the PDPC.

6.2 If such registration/notification is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?

This is not applicable in Singapore.

6.3 On what basis are registrations/notifications made (e.g., per legal entity, per processing purpose, per data category, per system or database)?

This is not applicable in Singapore.

Right to restrict processing

Please see our response to “Right to object to processing” above.

Right to data portability

Currently, this is not applicable in Singapore.

Recently, on 25 February 2019, the PDPC, in collaboration with the Competition and Consumer Commission of Singapore, published a paper discussing the benefits and issues that may arise with the introduction of a data portability requirement, including the potential impact on consumers, businesses and competition. However, it remains to be seen whether, and in what form, this data portability right will be introduced.

Right to withdraw consent

Please see our response to “Right to object to processing” above.

Right to object to marketing

Please see our response to “Right to object to processing” above.

In addition, an individual who does not wish to receive specified telemarketing calls and messages addressed to his Singapore telephone number may register his Singapore telephone number on one or more of the three DNC registers (namely, the No Call Register; the No Text Message Register; and the No Fax Message Register) (see our response to section 9.1 below).

Right to complain to the relevant data protection authority(ies)

An individual may lodge a complaint with the PDPC in respect of an organisation’s breach of any of the Data Protection Provisions or DNC Provisions. Upon receiving such a complaint, the PDPC may direct the individual and the organisation to: resolve the complaint; refer the matter for mediation; or conduct an investigation to determine whether or not the organisation is in compliance with the PDPA.

Other key rights – please specify

This is not applicable.

■ if the burden or expense of providing access would be unreasonable to the organisation or disproportionate to the individual’s interests;
■ for information that does not exist or cannot be found;
■ for information that is trivial; or
■ that is otherwise frivolous or vexatious.
In addition, Section 21(3) of the PDPA provides that an organisation shall not provide an individual with his personal data or other information, if doing so could be reasonably expected to:
■ threaten the safety or physical or mental health of an individual other than the individual who made the request;
■ cause immediate or grave harm to the safety or to the physical or mental health of the individual who made the request;
■ reveal personal data about another individual;
■ reveal the identity of an individual who has provided personal data about another individual and the individual providing the personal data does not consent to the disclosure of his identity; or
■ be contrary to the national interest.

Right to rectification of errors

Under Section 22 of the PDPA, an individual has the right to request an organisation to correct an error or omission in his personal data.
Specifically, an organisation is required to, on request by an individual: (a) correct an error or omission in the individual’s personal data that is in the possession or under the control of the organisation; and (b) send the corrected personal data to every other organisation to which the personal data was disclosed by the organisation within a year before the date the correction request was made, unless that other organisation does not need the corrected personal data for any legal or business purpose (“Correction Obligation”).
However, Section 22(7) of the PDPA provides that an organisation is not required to comply with the Correction Obligation in respect of the following matters specified in the Sixth Schedule to the PDPA:
■ opinion data kept solely for an evaluative purpose;
■ any examination conducted by an education institution, examination scripts and, prior to the release of examination results, examination results;
■ the personal data of the beneficiaries of a private trust kept solely for the purpose of administering the trust;
■ personal data kept by an arbitral institution or a mediation centre solely for the purposes of arbitration or mediation proceedings administered by the arbitral institution or mediation centre; and
■ a document related to a prosecution if all proceedings related to the prosecution have not been completed.
In addition, Section 22(6) of the PDPA provides that an organisation is not required to correct or otherwise alter an opinion, including a professional or an expert opinion.

Right to deletion/right to be forgotten

The PDPA does not accord an individual with the right to require an organisation to delete his personal data.

Right to object to processing

Under Section 16 of the PDPA, an individual may, upon giving reasonable notice to an organisation, withdraw his consent (which includes deemed consent) given to the organisation for the collection, use, or disclosure of his personal data for any purpose. Upon withdrawal of consent, the organisation must cease (and cause its data intermediaries and agents to cease) collecting, using or disclosing the personal data, as the case may be, unless the collection, use or disclosure of the personal data without consent is required or authorised under the PDPA or any other written law.

Right to restrict processing

Please see our response to “Right to object to processing” above.

Right to data portability

Currently, this is not applicable in Singapore.

Recently, on 25 February 2019, the PDPC, in collaboration with the Competition and Consumer Commission of Singapore, published a paper discussing the benefits and issues that may arise with the introduction of a data portability requirement, including the potential impact on consumers, businesses and competition. However, it remains to be seen whether, and in what form, this data portability right will be introduced.

Right to withdraw consent

Please see our response to “Right to object to processing” above.

Right to object to marketing

Please see our response to “Right to object to processing” above.

In addition, an individual who does not wish to receive specified telemarketing calls and messages addressed to his Singapore telephone number may register his Singapore telephone number on one or more of the three DNC registers (namely, the No Call Register; the No Text Message Register; and the No Fax Message Register) (see our response to section 9.1 below).

Right to complain to the relevant data protection authority(ies)

An individual may lodge a complaint with the PDPC in respect of an organisation’s breach of any of the Data Protection Provisions or DNC Provisions. Upon receiving such a complaint, the PDPC may direct the individual and the organisation to: resolve the complaint; refer the matter for mediation; or conduct an investigation to determine whether or not the organisation is in compliance with the PDPA.

Other key rights – please specify

This is not applicable.

- Right to rectification of errors
- Right to restrict processing
- Right to data portability
- Right to withdraw consent
- Right to object to marketing
- Right to complain to the relevant data protection authority(ies)
6.4 Who must register with/notify the data protection authority (e.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation)?

This is not applicable in Singapore.

6.5 What information must be included in the registration/notification (e.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes)?

This is not applicable in Singapore.

6.6 What are the sanctions for failure to register/notify where required?

This is not applicable in Singapore.

6.7 What is the fee per registration/notification (if applicable)?

This is not applicable in Singapore.

6.8 How frequently must registrations/notifications be renewed (if applicable)?

This is not applicable in Singapore.

6.9 Is any prior approval required from the data protection regulator?

This is not applicable in Singapore.

6.10 Can the registration/notification be completed online?

This is not applicable in Singapore.

6.11 Is there a publicly available list of completed registrations/notifications?

This is not applicable in Singapore.

6.12 How long does a typical registration/notification process take?

This is not applicable in Singapore.

7 Appointment of a Data Protection Officer

7.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.

The appointment of a Data Protection Officer is mandatory. Section 11(3) of the PDPA obliges an organisation to “designate one or more individuals to be responsible for ensuring that the organisation complies with [the PDPA].” The business contact information of at least one Data Protection Officer must be made available to the public.

7.2 What are the sanctions for failing to appoint a Data Protection Officer where required?

The PDPC may take the following enforcement actions against the organisation:
(a) give the organisation such directions as the PDPC thinks fit in the circumstances to ensure compliance; and/or
(b) require the organisation to pay a financial penalty of such amount not exceeding $1 million as the PDPC thinks fit.

For completeness, we note that the PDPC has actively enforced this requirement over the past year.

7.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect of his or her role as a Data Protection Officer?

The PDPA does not provide for any particular protections for Data Protection Officers in respect of their role as Data Protection Officers. However, it should be noted that the appointment of a Data Protection Officer does not relieve the organisation of its obligations and liabilities under the PDPA.

7.4 Can a business appoint a single Data Protection Officer to cover multiple entities?

Yes. Section 11(3) of the PDPA only provides that each organisation “shall designate one or more individuals to be responsible for ensuring that the organisation complies with [the PDPA],” but does not stipulate that organisations may not designate individuals already designated by other organisations. Section 11(4) of the PDPA further provides that an individual designated by an organisation may further delegate the responsibility conferred by that delegation to another individual. For the avoidance of doubt, the designated individual need not be an employee of the organisation.

7.5 Please describe any specific qualifications for the Data Protection Officer required by law.

There are no specific qualifications required by law of the Data Protection Officer. In practice, however, it would be advisable that an organisation appoint an individual (or a group of individuals) familiar with the data protection laws of Singapore, the organisation’s data protection policies and procedures, as well as its data processing activities. This is to ensure that the Data Protection Officer is well-equipped to: (i) ensure the organisation’s continued compliance with the PDPA; (ii) deal with any queries from authorities or the public in relation to the organisation’s data protection practices; and (iii) limit the impact of any data breach incident.

7.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?

The Data Protection Officer is responsible for ensuring the organisation’s continued compliance with the PDPA. However, it should be noted that the appointment of a Data Protection Officer does not relieve the organisation of its obligations and liabilities under the PDPA.
Some of the responsibilities of a Data Protection Officer may include, but are not limited to:
- ensuring compliance with the PDPA when developing and implementing policies and processes for handling personal data;
- fostering a data protection culture among employees and communicating personal data protection policies to stakeholders;
- managing personal data protection related queries and complaints;
- alerting management to any risks that might arise with regard to personal data; and
- liaising with the PDPC on data protection matters, if necessary.

7.7 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?

No, there is no requirement for the Data Protection Officer to be registered with or notified to the PDPC. However, DPOs are encouraged to register with the PDPC to keep abreast of developments in the PDPA.

7.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?

No. However, the business contact information of at least one Data Protection Officer must be made available to the public.

8 Appointment of Processors

8.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?

No. However, it should be noted that appointing a data intermediary to process personal data does not relieve the organisation of its obligations and liabilities under the PDPA, as the organisation is deemed to “have the same obligation under [the PDPA] in respect of personal data processed on its behalf and for its purposes by a data intermediary as if the personal data were processed by the organisation itself”.

Nonetheless, the Key Concepts Guidelines state that it is important that an organisation is clear as to its rights and obligations when dealing with another organisation and, where appropriate, include provisions in their written contracts to clearly set out each organisation’s responsibilities and liabilities in relation to the personal data in question, including whether one organisation is to process personal data on behalf of and for the purposes of the other organisation. If there is no contract evidenced or made in writing with the data organisation, the data intermediary will need to comply with all the Data Protection Provisions in respect of the personal data that is processed on behalf of the data organisation.

8.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?

As the organisation remains responsible for complying with the PDPA notwithstanding that a data intermediary is processing personal data on its behalf, it may be prudent for the organisation to impose specific obligations on its data intermediary through a written agreement, including restricting what the data intermediary may do with the disclosed personal data, having sufficient security measures to protect the disclosed personal data, and providing for audits, inspections, or other types of spot checks to satisfy itself that the data intermediary is complying with the PDPA.

9 Marketing

9.1 Please describe any legislative restrictions on the sending of electronic direct marketing (e.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?).

The PDPA and the SCA restrict the sending of unsolicited marketing communications by telephone, email, text messaging (be it via SMS or other messaging applications such as WhatsApp) and any other electronic communications.

Generally, where the personal data of an individual is collected, used and disclosed for marketing purposes, the consent of the individual concerned must be obtained and such consent must not have been obtained as a condition for the providing of a product or service where it would not be reasonably required to provide that product or service. This applies regardless of how the marketing communications are sent.

In this regard, the PDPC has noted in its Key Concepts Guidelines that a failure to opt out will not be regarded as consent in all situations, and has recommended that organisations obtain consent from an individual through a positive action of the individual. It would therefore be advisable to obtain prior opt-in consent instead.

In relation to the sending of marketing communications by telephone call or text messaging (or fax) to a Singapore telephone number, the PDPA requires an organisation to:

(a) verify against the relevant DNC Registry to confirm that the telephone number is not listed before sending the message or calling, unless clear and ambiguous consent to the sending of the specified message to that number is obtained in evidential form;
(b) include information identifying the sender for messages and details on how the sender can be readily contacted, and such details and contact information should be reasonably likely to be valid for at least 30 days after the sending of the message; and
(c) for voice calls, not conceal or withhold the calling line identity from the recipient.

In relation to the sending of unsolicited marketing communications in bulk by email or other electronic messages, Section 11 read with the Second Schedule of the SCA stipulates that such messages must contain, inter alia, the following:

(a) information on the sender;
(b) a clear and conspicuous statement in English setting out the procedure to unsubscribe;
(c) a title in its subject field that is reflective of the message’s content;
(d) a label “<ADV>” with a space before the title of the subject field, or in the absence of a title, the first word of the message; and
(e) header information that is not false or misleading; and
(f) an accurate and functional email address or telephone number by which the sender is readily contactable.

The unsubscribe facility must be legimitately obtained, and valid and capable of receiving the unsubscribe request and a reasonable
number of similar unsubscribe requests sent by other recipients at all times within at least 30 days after the unsolicited message is sent. No further unsolicited marketing communications can be sent after 10 business days following the date of the unsubscribe request. Furthermore, Section 9 of the SCA prohibits unsolicited commercial electronic messages in bulk from being sent to electronic addresses generated or obtained through the use of a dictionary attack or address-harvesting software.

9.2 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.).

Please see our response to section 9.1 above.

9.3 Do the restrictions noted above apply to marketing sent from other jurisdictions?

Yes, if the recipient of the marketing messages is present in Singapore when the marketing message is accessed. The PDPA applies to all organisations, whether or not formed or recognised under the laws of Singapore, or resident or having an office or a place of business in Singapore.

Specifically, the DNC provisions under the PDPA apply when the sender of the specified message is present in Singapore when the specified message is sent, or the recipient of the specified message is present in Singapore when the specified message is accessed. The SCA applies as long as the electronic message has a Singapore link, which includes, inter alia, the following situations:

- the message originates in Singapore or the sender of the message is, when the message is sent: (i) an individual who is physically present in Singapore; or (ii) an entity whose central management and control is in Singapore;
- the computer, mobile telephone, server or device that is used to access the message is located in Singapore; or
- the recipient of the message is, when the message is accessed: (i) an individual who is physically present in Singapore; or (ii) an entity that carries on business or activities in Singapore.

9.4 Is/are the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?

The PDPA is a complaints-based regime and the PDPC has been active in the enforcement of breaches thereof. Since the commencement of the PDPA in 2014, the PDPC has charged several individuals for offences relating to breaches of the DNC Registry.

9.5 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?

Purchasing marketing lists from third parties is only lawful if the individuals whose personal data is contained within the lists are notified of, and consent to, the sale of their personal data before such data are collected, used, and/or disclosed. The purchase of marketing lists constitutes collecting personal data under the PDPA. The PDPC has taken enforcement action against organisations which have purchased marketing lists without obtaining valid consent. For example, in the decision of Re Sharon Assya Qadriyah Tang [2018] SGPDPC 1, the PDPC imposed a financial penalty of S$6,000 on an individual for buying and selling marketing lists containing personal data.

9.6 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?

In relation to a breach of the Data Protection Provisions that apply to the sending of marketing communications, the organisation may find itself liable to pay a financial penalty of up to S$1 million.

In relation to the DNC Registry:

(a) For breaches of the obligation to check the DNC Registry, the offender would be guilty of an offence and liable on conviction to a fine not exceeding S$10,000.

(b) For breaches of the obligation to provide clear and accurate information identifying the sender and the sender’s contact details in the prescribed manner, the offender would be guilty of an offence and liable on conviction to a fine not exceeding S$10,000.

(c) For breaches of the obligation to provide the recipient with the calling line identity of the sender, the offender would be guilty of an offence and liable on conviction to a fine not exceeding S$10,000.

In appropriate cases, the PDPC may compound the offence for a sum of up to S$1,000. Whether composition is offered and the amount of composition will be decided by the PDPC based on the facts of each case.

These offences are in addition to the rights of private action that individuals may have against the organisation under the PDPA and SCA.

10 Cookies

10.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).

There are presently no legislative restrictions on the use of cookies or similar technologies per se, although the PDPA will apply to cookies that collect or use personal data.

According to the Advisory Guidelines on the PDPA for Selected Topics, for Internet activities that the user has clearly requested (e.g. transmitting personal data for effecting online communications and storing information that the user enters in a web form to facilitate an online purchase), there may not be a need to seek consent for the use of cookies to collect, use, and disclose personal data where the individual is aware of the purposes for such collection, use or disclosure and voluntarily provided his personal data for such purposes. For activities that cannot take place without cookies that collect, use or disclose personal data, consent may be deemed if the individual voluntarily provides the personal data for that purpose of the activity, and it is reasonable that he would do so.

Consent may also be reflected in the way a user configures his interaction with the Internet. If the individual configures his browser to accept certain cookies but rejects others, he may be found to have consented to the collection, use and disclosure of his personal data by the cookies that he has chosen to accept.
10.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?

This is not applicable in Singapore.

10.3 To date, has/have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?

To date, the PDPC has not issued any enforcement decisions specifically in relation to cookies.

10.4 What are the maximum penalties for breaches of applicable cookie restrictions?

This is not applicable in Singapore.

11 Restrictions on International Data Transfers

11.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.

The Transfer Limitation Obligation under the PDPA requires organisations transferring personal data abroad to do so only in accordance with the requirements prescribed under the PDPA to ensure that the recipients provide a standard of protection to personal data so transferred that is comparable to the protection under the PDPA.

In particular, under the PDPA Regulations, the transferring organisation must, before transferring the personal data outside of Singapore:

- take appropriate steps to ensure that the transferring organisation continues to comply with the Data Protection Provisions in respect of the personal data being transferred so long as such personal data remains in its possession or under its control; and
- take appropriate steps to ascertain whether, and to ensure that, the recipient is bound by legally enforceable obligations, to provide the personal data transferred with a standard of protection comparable to that provided for by the PDPA.

For completeness, the PDPA Regulations provide for certain prescribed situations whereby either or both of the above requirements are taken to be satisfied, e.g., where the personal data is publicly available in Singapore or where the personal data is in transit.

“Legally enforceable obligations” is defined in the PDPA Regulations to include obligations imposed on the recipient under:

(a) any law;
(b) any contract that requires the recipient to provide to the transferred personal data a standard of protection that is at least comparable to the protection under the PDPA, and which specifies the countries and territories to which the personal data may be transferred under the contract;
(c) any binding corporate rules (in cases where a recipient is an organisation related to the transferring organisation) that require every employee or person to provide to the transferred personal data a standard of protection that is at least comparable to the protection under the PDPA, and which specifies (i) the recipients of the transferred personal data to which the binding corporate rules apply, (ii) the countries and territories to which the personal data may be transferred under the binding corporate rules, and (iii) the rights and obligations provided by the binding corporate rules; or
(d) any other legally binding instrument.

The Regulations define a recipient as being related to the transferring organisation if:

(a) the recipient, directly or indirectly, controls the transferring organisation;
(b) the recipient is, directly or indirectly, controlled by the transferring organisation; or
(c) the recipient and the transferring organisation are, directly or indirectly, under the control of a common person.

11.2 Please describe the mechanisms businesses typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).

Companies generally rely on robust data transfer agreements and binding corporate rules, as well as active enforcement of the terms of these documents, to ensure their compliance with applicable transfer restrictions.

11.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.

No, there is no requirement for the registration/notification or prior approval from the PDPC for transfers of personal data abroad.

12 Whistle-blower Hotlines

12.1 What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?

The PDPA does not specifically regulate corporate whistle-blowing hotlines. To the extent that whistle-blowing falls under the definition of “investigation” as found in the PDPA, the PDPA provides that personal data can be collected without obtaining consent if it is necessary for any investigation or proceedings, and it is reasonable to expect that seeking the consent of the individual would compromise the availability or the accuracy of the personal data. Similarly, the use and disclosure of personal data can be done without obtaining consent if it is necessary for any investigation or proceedings.

In this regard, the PDPA defines “investigation” to refer to an investigation relating to:

(a) a breach of an agreement;
(b) a contravention of any written law, or any rule of professional conduct or other requirement imposed by any regulatory authority in exercise of its powers under any written law; or
(c) a circumstance or conduct that may result in a remedy or relief being available under any law.
12.2 Is anonymous reporting prohibited, strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do businesses typically address this issue?

Anonymous reporting is not regulated under the PDPA.

13 CCTV

13.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?

The PDPA does not require the use of CCTV to be separately registered/notified or approved beforehand by the PDPC. However, as video and audio recordings of individuals may constitute personal data, the use of CCTV may constitute the collection of personal data and hence an organisation must comply with the PDPA when using CCTV.

Notices or other forms of notifications should generally be placed at locations that would enable individuals to have sufficient awareness that CCTV has been deployed for a particular purpose.

13.2 Are there limits on the purposes for which CCTV data may be used?

Insofar as CCTV data contains personal data, the PDPA limits the purposes for which the CCTV data may be used.

14 Employee Monitoring

14.1 What types of employee monitoring are permitted (if any), and in what circumstances?

Employee monitoring is not specifically regulated in Singapore. To the extent that the employee monitoring overlaps with the employer’s obligations under the PDPA, such monitoring will fall to be regulated by the Data Protection Provisions.

14.2 Is consent or notice required? Describe how employers typically obtain consent or provide notice.

Before collecting, using or disclosing the personal data (which would include CCTV images/footage of such employees and the other data collected by the employer pursuant to their employee monitoring activities, to the extent that the employees can be identified from such data) of their employees, employers are generally required to provide suitable notices and obtain consent.

An exception to this requirement under the PDPA is where personal data is collected by the employer and the collection is reasonable for the purpose of managing or terminating an employment relationship.

Due to the inherent uncertainty of the ambit of this exception, it is common for employers to include related clauses in their personal data protection policies, employment handbook or their employment agreements to obtain express consent from their employees prior to the commencement of employee monitoring or using CCTV surveillance. It is also not unusual for organisations to provide prominent notices at the entrances of their premises to alert visitors that their premises are monitored by CCTV. Such notices should state the purpose of the CCTV.

14.3 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?

As the relationship between employers and trade unions are very much subject to the terms of the collective agreement, the necessity of notifying or consulting the trade unions in respect of CCTV and employee monitoring is dependent on the terms of the collective agreement. There are generally no legal requirements under Singapore law requiring works councils/trade unions/employee representatives to be notified or consulted.

15 Data Security and Data Breach

15.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?

Yes, both organisations and data intermediaries are subject to the Protection Obligation in relation to the personal data in their possession or control. For the Protection Obligation, please see our response to section 4.1 above.

While the PDPC has recognised that there is no one-size-fits-all solution, it has, in its Key Concepts Guidelines, noted that an organisation should:

- design and organise its security arrangements to fit the nature of the personal data held by the organisation and the possible harm that might result from a security breach;
- identify reliable and well-trained personnel responsible for ensuring information security;
- implement robust policies and procedures for ensuring appropriate levels of security for personal data of varying levels of sensitivity; and
- be prepared and able to respond to information security breaches promptly and effectively.

15.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

There is currently no mandatory requirement under the PDPA for organisations to report data breaches to the PDPC. However, the PDPC recommends that organisations provide notification to the PDPC as soon as possible of any data breaches that might cause public concern, or where there is a risk of harm to a group of affected individuals, or where the data breach involves sensitive personal data.

According to the Enforcement Guidelines, the fact that an organisation has voluntarily notified the PDPC of a data breach as soon as it learned of the breach, and cooperated with the PDPC in its investigations may be a mitigating factor that the PDPC will take into account when calculating the financial penalty.

The notification can be sent to the PDPC via email (info@pdpc.gov.sg with the subject title “[Data Breach Notification]”), or via phone for urgent notification of major cases (+65 6377 3131). It should include information such as the following:
Individuals may be liable to a fine of up to S$10,000.

Enforcement and Sanctions

There is currently no mandatory requirement under the PDPA for organisations to notify individuals of data breaches. However, an organisation may need to provide such notification to individuals pursuant to its other legal or contractual obligations.

The PDPC has also recommended that organisations should notify individuals affected by a data breach as a matter of best practice. Such notification should also be provided to parents or guardians of young children whose personal data have been compromised, third parties such as banks, credit card companies or the police (where relevant).

15.3 Is there a legal requirement to report data breaches to affected data subjects? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

As set out in the Enforcement Guidelines, the factors are considered by the PDPC to be mitigating factors:

- the organisation took immediate steps to notify affected individuals of the breach and reduce the damage caused by a breach (such as informing individuals of steps they can take to mitigate risk); and
- the organisation has engaged the individual in a meaningful manner and has voluntarily offered a remedy to the individual, and that individual has accepted the remedy.

15.4 What are the maximum penalties for data security breaches?

The PDPC has discretion to issue such remedial directions as it thinks fit, including a direction to require payment of a financial penalty of up to S$1 million.

On 15 January 2019, the PDPC imposed its highest financial penalties to date of S$250,000 and S$750,000 respectively on SingHealth Services Pte Ltd (“SingHealth”) and Integrated Health Information Systems Pte Ltd, for breaching their data protection obligations under the PDPA. This unprecedented data breach which arose from a cyber attack on SingHealth’s patient database system caused the personal data of some 1.5 million patients to be compromised.

16 Enforcement and Sanctions

16.1 Describe the enforcement powers of the data protection authority(ies).

<table>
<thead>
<tr>
<th>Investigatory Power</th>
<th>Civil/Administrative Sanction</th>
<th>Criminal Sanction</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power to require documents or information.</td>
<td>Not applicable.</td>
<td>Individuals may be liable to a fine of up to S$10,000 and imprisonment for a term of up to 12 months, or both; whereas organisations may be liable to a fine of up to S$100,000 for providing any false or misleading statements or information to the PDPC.</td>
</tr>
<tr>
<td>Power to enter premises with or without a Court-issued search warrant.</td>
<td>Not applicable.</td>
<td>Individuals may be liable to a fine of up to S$10,000 and imprisonment for a term of up to 12 months, or both; whereas organisations may be liable to a fine of up to S$100,000 for obstructing or hindering the PDPC.</td>
</tr>
<tr>
<td>Power to review, on application of a complainant: (i) refusals to provide access to personal data requested by the complainant under the PDPA or a failure to provide such access within a reasonable time; (ii) a fee required from the complainant by an organisation in relation to a request by the complainant under the PDPA; or (iii) refusals to correct personal data in accordance with a request by the complainant under the PDPA.</td>
<td>The PDPC may: (i) confirm the refusal to provide access to or correct the personal data (as the case may be) and direct the organisation to provide access to or correct the personal data (as the case may be) within a specified timeframe; or (ii) confirm, reduce or disallow a fee, or direct the organisation to make a refund to the complainant.</td>
<td>Not applicable.</td>
</tr>
</tbody>
</table>
The PDPC may issue such directions as it thinks fit in the circumstances to ensure compliance by an organisation with the Data Protection Provisions under Parts III to VI of the PDPA. These include directions to: (i) stop collecting, using or disclosing personal data in contravention of the PDPA; (ii) destroy personal data collected in contravention of the PDPA; (iii) comply with any direction of the PDPC; and (iv) pay a financial penalty of up to S$1 million.

<table>
<thead>
<tr>
<th>Investigatory Power</th>
<th>Civil/Administrative Sanction</th>
<th>Criminal Sanction</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power to give directions.</td>
<td>The PDPC may issue such directions as it thinks fit in the circumstances to ensure compliance by an organisation with the Data Protection Provisions under Parts III to VI of the PDPA. These include directions to: (i) stop collecting, using or disclosing personal data in contravention of the PDPA; (ii) destroy personal data collected in contravention of the PDPA; (iii) comply with any direction of the PDPC; and (iv) pay a financial penalty of up to S$1 million.</td>
<td>Not applicable.</td>
</tr>
</tbody>
</table>

16.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?

The PDPC is empowered to direct an organisation to stop collecting, using, or disclosing personal data in contravention of the PDPA. The PDPC does not require a court order to issue directions. Nonetheless, the PDPC may apply for the direction to be registered in a District Court for the purposes of enforcement by the court.

16.3 Describe the data protection authority's approach to exercising those powers, with examples of recent cases.

The PDPC takes a pragmatic approach in administering and enforcing the PDPA and aims to balance the need to protect individuals’ personal data and the needs of organisations to use the data for legitimate purposes.

Over the past year (2018), the PDPC has published more than 20 enforcement decisions with a significant majority of these cases relating to breaches of the Protection Obligation. In respect of these cases, the PDPC has either issued a warning or imposed directions requiring the infringing organisation to take remedial action and to pay financial penalties, although there were some cases where no breaches of the PDPA were found.

Examples of recent cases include:

- **Breach of Protection Obligation by GrabCar**: A financial penalty of S$6,000 was imposed on GrabCar, for failing to properly configure a Google Forms document used to collect the personal data of drivers, resulting in the inadvertent disclosure of the personal data to subsequent users of the document.
- **Breach of Protection Obligation by Jade E-Services**: A warning was issued to Jade E-Services for failing to implement proper and adequate security measures on an e-commerce website it administered, resulting in the personal data of one user being accidentally disclosed to another user.
- **Breach of Protection Obligation by Sharon Assy Qadriyah Tang**: A financial penalty of S$6,000 was issued to an individual who had bought and sold marketing lists, in the first case involving the selling of personal data.
- **Breach of Consent and Purpose Limitation Obligations by Spring College International**: The PDPC issued directions to an educational institution to remove posts containing the personal data of its students from its social media pages, and to revise the consent forms signed by students to specifically consent to the use of their personal data for marketing purposes.

16.4 Does the data protection authority ever exercise its powers against businesses established in other jurisdictions? If so, how is this enforced?

We have not sighted a published decision whereby the PDPC has exercised its powers against companies established in other jurisdictions with no presence in Singapore.

Nonetheless, the PDPC is empowered to enter into a cooperation agreement with a foreign data protection authority for data protection matters such as cross-border cooperation. Specifically, under Section 10 of the PDPA, cooperation agreements may be entered into for the purposes of:

- facilitating cooperation between the PDPC and another foreign data protection authority in the performance of their respective functions insofar as those functions relate to data protection; and
- avoiding duplication of activities by the PDPC and another foreign data protection authority, being activities involving the enforcement of data protection laws.

The PDPC may also furnish information to a foreign data protection body pursuant to a cooperation agreement, subject to the fulfilment of certain prescribed conditions.

The PDPC is also a participant of the Asia Pacific Economic Corporation (“APEC”) Cross-border Privacy Enforcement Arrangement, which creates a framework for the voluntary sharing of information and provision of assistance for privacy enforcement-related activities.

17 E-discovery / Disclosure to Foreign Law Enforcement Agencies

17.1 How do businesses typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?

Generally, organisations must ensure that any transfers of personal data outside of Singapore comply with the requirements under the PDPA (see our response to section 11 above). It is not uncommon for Singapore businesses to include, in their privacy policy, a general notice that any personal data they collect may be disclosed to foreign law enforcement agencies or in relation to investigations and legal proceedings.

17.2 What guidance has/have the data protection authority(ies) issued?

The PDPC has not issued any specific guidance yet in relation to foreign e-discovery requests or requests for disclosure from foreign law enforcement agencies.

18 Trends and Developments

18.1 What enforcement trends have emerged during the previous 12 months? Describe any relevant case law.

Breaches of the Protection Obligation under the PDPC continue to constitute the majority of enforcement decisions issued by the PDPC, with 22 out of 30 cases over the past 12 months involving the Protection Obligation. Instances where businesses have been found to have inadequate privacy policies in place have decreased,
18.2 What “hot topics” are currently a focus for the data protection regulator?

APEC CBPR
On 20 February 2018, Singapore became the sixth APEC economy to participate in the APEC Cross-Border Privacy Rules (“CBPR”) system, along with the USA, Mexico, Canada, Japan and the Republic of Korea. Singapore also became the second APEC economy to participate in the APEC Privacy Recognition for Processors (“PRP”) system. Collectively, the CBPR and PRP systems allow a smoother exchange of personal data among certified organisations in participating economies, and ensure that data protection standards are maintained for consumers in the Asia-Pacific region.

Data Protection Trustmark Certification Scheme
On 9 January 2019, IMDA launched the Data Protection Trustmark certification scheme for the CBPR and PRP systems, which was developed by the PDPC. The certification establishes a robust data governance standard to help businesses increase their competitive advantage and build trust with their customers. Once the certification scheme is implemented, organisations may start applying for certification under the relevant systems.

Model Artificial Intelligence (“AI”) Governance Framework
On 23 January 2019, the PDPC issued a Proposed Model Artificial Intelligence Governance Framework for public consultation and pilot adoption. The accountability-based framework helps chart the language and frame the discussions around harnessing AI in a responsible way. The framework is intended to assist organisations to achieve the following objectives: (a) build consumer confidence in AI through organisations’ responsible use of such technologies to mitigate different types of risks in AI deployment; and (b) demonstrate reasonable efforts to align internal policies, structures and processes with relevant accountability-based practices in data management and protection, e.g. the PDPA and OECD Privacy Principles.

Discussion Paper on Data Portability
On 25 February 2019, the PDPC, together with the Competition and Consumer Commission of Singapore, published a Discussion Paper on Data Portability. Essentially, the data portability requirement is the ability of individuals to request from an organisation a copy of their personal data held by that organisation in a structured, machine-readable format, so that another organisation may make use of their personal data. The discussion paper sets out how data portability supports business innovation and drives competition while simultaneously empowering consumers by giving them greater flexibility and control over their personal data. It also provides a framework for stakeholders to understand and further discuss the operational considerations in implementing a data portability requirement.

Lim Chong Kin
Drew & Napier LLC
10 Collyer Quay
10th Floor, Ocean Financial Centre
Singapore 049315

Tel: +65 6531 4110
Email: chongkin.lim@drewnapier.com
URL: www.drewnapapier.com

Chong Kin heads Drew & Napier’s Telecommunications, Media and Technology Practice Group.

Under Chong Kin’s leadership, the Practice Group is consistently ranked as the leading practice in Singapore. His clients include the telecoms and media regulators, global carriers, technology market leaders, global broadcasters and content providers.

Chong Kin has been an external legal and regulatory advisor for the Personal Data Protection Commission of Singapore since 2013, and he played a key role in the liberalisation of Singapore’s telecoms, media and postal sectors where he drafted the competition frameworks.

Chong Kin is highly regarded by his peers, clients and rivals alike for his expertise, and is consistently recommended as a leading lawyer by major international legal publications such as Chambers Asia-Pacific, The Legal 500 Asia Pacific, Who’s Who Legal, The Guide to the World’s Leading Competition & Antitrust Lawyers/Economists, Global Competition Review, Practical Law Company – Which Lawyer?, Asialaw Profiles and Best Lawyers.
Chapter 40

Spain

Ecija Abogados

Carlos Pérez Sanz

Pia Lestrade Dahms

1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?
Since 25 May 2018, the principal data protection legislation in the EU has been Regulation (EU) 2016/679 (the “General Data Protection Regulation” or “GDPR”). The GDPR repealed Directive 95/46/EC (the “Data Protection Directive”) and has led to increased (though not total) harmonisation of data protection law across the EU Member States.

Since 7 December 2018, Spanish Law 3/2018 on Personal Data Protection and Digital Rights (the “LOPD” or “Law 3/2018”) is also applicable.

1.2 Is there any other general legislation that impacts data protection?

Organic Law 1/1982 on civil protection of the rights to honour, personal and family privacy and an individual’s own image.

Gross privacy non-disclosure violations might be prosecuted under criminal charges in accordance with Art. 197 of the Criminal Code.

Law 34/2002 on information society services and ecommerce (the “LSSI”). This law covers the e-marketing communications regime, internet service provider (ISP) liability and anti-spam regulation.

1.3 Is there any sector-specific legislation that impacts data protection?

A large number of sector-specific legislation is available. A few examples are listed below:

(a) Art. 96 of the Spanish Consumer Rights Act Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias, in connection with Art. 29 of Ley 3/1991 de 10 de enero, de competencia desleal, as modified by Law 29/2009. According to this regulation, marketing phone calls must be clearly identified as such, and fully disclose the identity of the calling company. In every communication, recipients shall be offered the opportunity to oppose further calling. Human operators are allowed for telemarketing only. Recorded telemarketing campaigns need the prior recipient to opt-in.

(b) Art. 41 of the Spanish Telecoms Act Ley 9/2014, de mayo, General de Telecomunicaciones sets forth privacy standards for telecommunications, including compulsory notifications to the Data Protection Authority (the “DPA”) and to data subjects in the case of breaches or violations of security. Art. 48 further provides that customers’ geolocation information (latitude data) should always be processed anonymously. Nominal customer geolocation is only allowed when strictly necessary and indispensable for the provision of value-added services expressly requested by the customer. In such a case, the customer should be informed about the extent, purpose and duration of this processing.

(c) Insurance legislation such as Real Decreto Legislativo 6/2004, de 29 de octubre, por el que se aprueba el texto refundido de la Ley de ordenación y supervisión de los seguros privados and Ley 26/2006, de 17 de julio, de medición de seguros y reaseguros privados contains data protection provisions specific to the insurance industry.

(d) Legislation specific to healthcare service provisions sheds light on rights to access health records and mandatory conservation timeframes of such information. The most important piece of legislation is Ley 41/2002, de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica.

(e) Art. 17 of Ley 59/2003 de firma electrónica covers data privacy issues related to electronic signatures.

(f) Real Decreto 1553/2005, de 23 diciembre, por el que se regula la expedición del documento nacional de identidad y sus certificados de firma electrónica covers electronic identity card usage.

(g) Art. 6.2b of Ley 11/2007 de Acceso electrónico de los ciudadanos a los servicios públicos provides the citizens’ right to get in touch with the public administration by electronic means. It has now been derogated by Ley 39/2015, de 1 octubre, del Procedimiento administrativo común de las administraciones públicas. The public administration must ensure security measures when handling a citizen’s data with regards to such communication.

(h) The Spanish Data Retention Act Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones. This act governs carrier companies’ obligations to retain traffic and personal data related to such traffic.

(i) Art. 20.3 of Real Decreto Legislativo 2/2015, de 23 de octubre, del Estatuto de los Trabajadores. This Article sets out that control measures on employees are permitted.
1.4 What authority(ies) are responsible for data protection?

The main data protection authority is the Agencia Española de Protección de Datos (the “AEPD”). However, there are also regional data protection authorities in Catalonia and the Basque Country with powers essentially over public entities within their respective territory.

2 Definitions

2.1 Please provide the key definitions used in the relevant legislation:

- “Personal Data” means any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

- “Processing” means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

- “Controller” means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

- “Processor” means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

- “Data Subject” means an individual who is the subject of the relevant personal data.

- “Sensitive Personal Data” are personal data, revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, data concerning health or sex life and sexual orientation, genetic data or biometric data.

- “Data Breach” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Other key definitions – please specify (e.g., “Pseudonymous Data”, “Direct Personal Data”, “Indirect Personal Data”). There are no other key definitions to be aware of.

3 Territorial Scope

3.1 Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to those laws?

The GDPR applies to businesses that are established in any EU Member State, and that process personal data (either as a controller or processor, and regardless of whether or not the processing takes place in the EU) in the context of that establishment.

A business that is not established in any Member State, but is subject to the laws of a Member State by virtue of public international law, is also subject to the GDPR.

The GDPR applies to businesses outside the EU if they (either as controller or processor) process the personal data of data subjects who are in the EU in relation to: (i) the offering of goods or services (whether or not in return for payment) to data subjects who are in the EU; or (ii) the monitoring of the behaviour of data subjects who are in the EU (to the extent that such behaviour takes place in the EU).

Further, the GDPR applies to businesses established outside the EU if they monitor the behaviour of data subjects who are in the EU (to the extent such behaviour takes place in the EU).

4 Key Principles

4.1 What are the key principles that apply to the processing of personal data?

- **Transparency**
  
  Personal data must be processed lawfully, fairly and in a transparent manner. Controllers must provide certain minimum information to data subjects regarding the collection and further processing of their personal data. Such information must be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

- **LAWFUL BASIS FOR PROCESSING**
  
  Processing of personal data is lawful only if, and to the extent that, it is permitted under EU data protection law. The GDPR provides an exhaustive list of legal bases on which personal data may be processed, of which the following are the most relevant for businesses: (i) prior, freely given, specific, informed and unambiguous consent of the data subject; (ii) contractual necessity (i.e., the processing is necessary for the performance of a contract to which the data subject is a party, or for the purposes of pre-contractual measures taken at the data subject’s request); (iii) compliance with legal obligations (i.e., the controller has a legal obligation, under the laws of the EU or an EU Member State, to perform the relevant processing); or (iv) legitimate interests (i.e., the processing is necessary for the purposes of legitimate interests pursued by the controller, except where the controller’s interest are overridden by the interests, fundamental rights or freedoms of the affected data subjects).

  Please note that businesses require stronger grounds to process sensitive personal data. The processing of sensitive personal data is only permitted under certain conditions, of which the most relevant for businesses are: (i) explicit consent of the affected data subject; (ii) the processing is necessary in the context of employment law; or (iii) the processing is necessary for the establishment, exercise or defence of legal claims.

- **Purpose limitation**

  Personal data may only be collected for specified, explicit and legitimate purposes and must not be further processed in a manner that is incompatible with those purposes. If a controller wishes to use the relevant personal data in a manner that is incompatible with the purposes for which they were initially collected, it must: (i) inform the data subject of such new processing; and (ii) must be able to rely on a lawful basis as set out above.

- **Data minimisation**

  Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which those data
are processed. A business should only process the personal data that it actually needs to process in order to achieve its processing purposes.

- **Proportionality**
  Not applicable.

- **Retention**
  Personal data must be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

- **Data security**
  Personal data must be processed in a manner that ensures appropriate security of those data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

- **Accountability**
  The controller is responsible for, and must be able to demonstrate, compliance with the data protection principles set out above.

- **Accuracy**
  Personal data must be accurate and, where necessary, kept up to date. A business must take every reasonable step to ensure that personal data that are inaccurate are either erased or rectified without delay.

### 5 Individual Rights

#### 5.1 What are the key rights that individuals have in relation to the processing of their personal data?

- **Right of access to data/copies of data**
  A data subject has the right to obtain from a controller the following information in respect of the data subject’s personal data: (i) confirmation of whether, and where, the controller is processing the data subject’s personal data; (ii) information about the purposes of the processing; (iii) information about the categories of data being processed; (iv) information about the categories of recipients with whom the data may be shared; (v) information about the period for which the data will be stored (or the criteria used to determine that period); (vi) information about the existence of the rights to erasure, to rectification, to restriction of processing and to objection to processing; (vii) information about the existence of the right to complain to the relevant data protection authority; (viii) where the data were not collected from the data subject, information as to the source of the data; and (ix) information about the existence of, and an explanation of the logic involved in, any automated processing that has a significant effect on the data subject.

  Additionally, the data subject may request a copy of the personal data being processed.

- **Right to rectification of errors**
  Controllers must ensure that inaccurate or incomplete data are erased or rectified. Data subjects have the right to rectification of inaccurate personal data.

- **Right to deletion/right to be forgotten**
  Data subjects have the right to erasure of their personal data (the “right to be forgotten”) if: (i) the data are no longer needed for their original purpose (and no new lawful purpose exists); (ii) the lawful basis for the processing is the data subject’s consent, the data subject withdraws that consent, and no other lawful ground exists; (iii) the data subject exercises the right to object, and the controller has no overriding grounds for continuing the processing; (iv) the data have been processed unlawfully; or (v) erasure is necessary for compliance with EU law or national data protection law.

- **Right to object to processing**
  Data subjects have the right to object, on grounds relating to their particular situation, to the processing of personal data where the basis for that processing is either public interest or legitimate interest of the controller. The controller must cease such processing unless it demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the relevant data subject or requires the data in order to establish, exercise or defend legal rights.

- **Right to restrict processing**
  Data subjects have the right to restrict the processing of personal data, which means that the data may only be held by the controller, and may only be used for limited purposes if: (i) the accuracy of the data is contested (and only for as long as it takes to verify that accuracy); (ii) the processing is unlawful and the data subject requests restriction (as opposed to exercising the right to erasure); (iii) the controller no longer needs the data for their original purpose, but the data are still required by the controller to establish, exercise or defend legal rights; or (iv) verification of overriding grounds is pending, in the context of an erasure request.

- **Right to data portability**
  Data subjects have the right to receive a copy of their personal data in a commonly used machine-readable format, and transfer their personal data from one controller to another or have the data transmitted directly between controllers.

- **Right to withdraw consent**
  A data subject has the right to withdraw their consent at any time. The withdrawal of consent does not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject must be informed of the right to withdraw consent. It must be as easy to withdraw consent as to give it.

- **Right to object to marketing**
  Data subjects have the right to object to the processing of personal data for the purpose of direct marketing, including profiling.

- **Right to complain to the relevant data protection authority(ies)**
  Data subjects have the right to lodge complaints concerning the processing of their personal data with the applicable data protection authority, if the data subjects live in Spain or the alleged infringement occurred in Spain.

  **Other key rights – please specify**

- **Right to information**
  Data subjects have the right to be provided with information on the identity of the controller, the reasons for processing their personal data and other relevant information necessary to ensure the fair and transparent processing of personal data.

  Spanish Law 3/2018 provides that it is possible to comply with the right to information via a layered approach: providing a first layer with some basic information on personal data protection (see Article 11 of said law for the minimum content that must be provided) and indicating how the data subject may access the complete information.
### Registration Formalities and Prior Approval

**6.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?**

There was a general requirement under the former data protection law in Spain to register with/notify the Spanish data protection authority before creating files containing personal data (as well as to notify any modifications or cancellations of such files). This is no longer the case with Law 3/2018.

However, entities responsible for advertisement exclusion systems must notify the data protection authority of their creation, whether they are general or sector-specific, as well as the method for data subjects to be included in them, and, where applicable, indicate their preferences (see Article 23 of Law 3/2018).

**6.2 If such registration/notice is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?**

See the answer to question 6.1.

**6.3 On what basis are registrations/notifications made (e.g., per legal entity, per processing purpose, per data category, per system or database)?**

See the answer to question 6.1.

**6.4 Who must register with/notify the data protection authority (e.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation)?**

See the answer to question 6.1.

**6.5 What information must be included in the registration/notification (e.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes)?**

See the answer to question 6.1.

**6.6 What are the sanctions for failure to register/notify where required?**

See the answer to question 6.1.

**6.7 What is the fee per registration/notification (if applicable)?**

See the answer to question 6.1.

**6.8 How frequently must registrations/notifications be renewed (if applicable)?**

See the answer to question 6.1.

**6.9 Is any prior approval required from the data protection regulator?**

See the answer to question 6.1.

**6.10 Can the registration/notification be completed online?**

See the answer to question 6.1.

**6.11 Is there a publicly available list of completed registrations/notifications?**

See the answer to question 6.1.

**6.12 How long does a typical registration/notification process take?**

See the answer to question 6.1.

### Appointment of a Data Protection Officer

**7.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.**

The appointment of a Data Protection Officer for controllers or processors is only mandatory in some circumstances, including where there is: (i) large-scale regular and systematic monitoring of individuals; or (ii) large-scale processing of sensitive personal data.

Where a business designates a Data Protection Officer voluntarily, the requirements of the GDPR apply as though the appointment were mandatory.

Please note that Spanish Law 3/2018 provides an extensive list of when the appointment of a Data Protection Officer is mandatory:

- Professional associations and their general councils.
- Educational centres that offer education at any of the levels established in the legislation regulating the right to education, as well as public and private universities.
- Entities that operate networks and provide electronic communications services in accordance with the provisions of their specific legislation, when they regularly and systematically process personal data on a large scale.
- Society information service providers when they elaborate/create profiles of users of the service on a large scale.
- Entities included in Article 1 of Law 10/2014, of 26 June, on the organisation, supervision and solvency of credit institutions.
- Credit institutions.
- Insurance and reinsurance entities.
- Investment services companies, regulated by the Securities Market legislation.
- Distributors and marketers of electric power and natural gas.
Entities responsible for general files for assessing asset and credit solvency or common files for the management and prevention of fraud, including those responsible for the files regulated by the legislation on the prevention of money laundering and financing of terrorism.

- Entities engaged in advertising activities and commercial research, including commercial and market research, when they carry out processing activities based on preferences of data subjects or when they carry out processing activities which involve profiling data subjects.
- Health centres that are legally required to keep medical records of patients (except certain health professionals).
- Entities whose purpose includes the issuance of commercial reports which may concern natural persons.
- Gaming operators whose activity is carried out electronically, telematically and interactively, in accordance with the gaming regulation.
- Private security companies.
- Sports federations when they process data of minors.

7.2 What are the sanctions for failing to appoint a Data Protection Officer where required?

In the circumstances where appointment of a Data Protection Officer is mandatory, failure to comply may result in the wide range of penalties available under the GDPR.

Yes, the controller or processor must notify the data protection authority of the contact details of the designated Data Protection Officer.

More specifically, Spanish Law 3/2018 provides that controllers and processors shall notify designations and dismissals of Data Protection Officers to the relevant data protection authority within 10 days. This applies when the designation of a Data Protection Officer is mandatory as well as when the entity chooses to appoint one voluntarily.

7.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect of his or her role as a Data Protection Officer?

The appointed Data Protection Officer should not be dismissed or penalised for performing their tasks and should report directly to the highest management level of the controller or processor.

The Data Protection Officer does not necessarily need to be named in the public-facing privacy notice. However, the contact details of the Data Protection Officer must be notified to the data subject when personal data relating to that data subject are collected. As a matter of good practice, the Article 29 Working Party (the “WP29”) (now the European Data Protection Board (the “EDPB”)) recommended in its 2017 guidance on Data Protection Officers that both the data protection authority and employees should be notified of the name and contact details of the Data Protection Officer.

The AEPD’s list of DPOs is available at the following link: https://sedeagpd.gob.es/sede-electronica-web/vistas/infoSede/consultaDPD.jsf

7.4 Can a business appoint a single Data Protection Officer to cover multiple entities?

A single Data Protection Officer is permitted by a group of undertakings provided that the Data Protection Officer is easily accessible from each establishment.

7.5 Please describe any specific qualifications for the Data Protection Officer required by law.

The Data Protection Officer should be appointed on the basis of professional qualities and should have an expert knowledge of data protection law and practices. While this is not strictly defined, it is clear that the level of expertise required will depend on the circumstances. For example, the involvement of large volumes of sensitive personal data will require a higher level of knowledge.

7.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?

A Data Protection Officer should be involved in all issues which relate to the protection of personal data. The GDPR outlines the minimum tasks required by the Data Protection Officer which include: (i) informing the controller, processor and their relevant employees who process data of their obligations under the GDPR; (ii) monitoring compliance with the GDPR, national data protection legislation and internal policies in relation to the processing of personal data including internal audits; (iii) advising on data protection impact assessments and the training of staff; and (iv) co-operating with the data protection authority and acting as the authority’s primary contact point for issues related to data processing.

7.7 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?

Yes, the controller or processor must notify the data protection authority of the contact details of the designated Data Protection Officer.

8 Appointment of Processors

8.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?

Yes. A business that appoints a processor to process personal data on its behalf is required to enter into an agreement with the processor which sets out the subject matter for processing, the duration of processing, the nature and purpose of processing, the types of personal data and categories of data subjects and the obligations and rights of the controller (i.e., the business).

It is essential that the processor appointed by the business complies with the GDPR.
Please note that Spanish Law 3/2018 has a specific transition clause regarding data processing contracts. This clause provides that data processing contracts entered into before 25 May 2018 will remain valid until their termination date. Where the contract has been entered into for an indefinite term, it will remain valid until 25 May 2022. Notwithstanding the foregoing, any of the parties may request, within those time periods, that the data processing contract be modified in order to comply with the GDPR.

However, it is recommended to modify existing data processing contracts to comply with the GDPR.

8.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?

The processor must be appointed under a binding agreement in writing. The contractual terms must stipulate that the processor: (i) only acts on the documented instructions of the controller; (ii) imposes confidentiality obligations on all employees; (iii) ensures the security of personal data that it processes; (iv) abides by the rules regarding the appointment of sub-processors; (v) implements measures to assist the controller with guaranteeing the rights of data subjects; (vi) assists the controller in obtaining approval from the relevant data protection authority; (vii) either returns or destroys the personal data at the end of the relationship (except as required by EU or Member State law); and (viii) provides the controller with all information necessary to demonstrate compliance with the GDPR.

9 Marketing

9.1 Please describe any legislative restrictions on the sending of electronic direct marketing (e.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?).

Unsolicited Email, SMS and Other Electronic Means

General opt-in rule: Unsolicited emailing requires previous opting in from the data subject.

Exceptional opt-out rule: Customers can be sent unsolicited emails, provided such unsolicited emailing is advertising similar goods and services to those previously purchased by such customers.

Single click unsubscribe: Such an option at the end of every post is mandatory.

The Robinson List: Must be checked before sending electronic communications.

9.2 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.).

Regular Post

Unsolicited marketing communications can only be sent in written paper format by regular post to individuals whose contact details are displayed in telephone directories or are obtained from other public sources.

Phone Call

The Spanish Consumer Rights Act Real Decreto Legislativo 1/2007, de 16 de noviembre, po el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias bans “robot” telemarketing phone calls. Unsolicited telemarketing calls must be performed by human agents, and shall always show the phone number of the calling party. People in the Robinson List should never be contacted.

Art. 29 of the Spanish Unfair Competition Act Ley 3/1991, de 10 de enero, de Competencia Desleal considers it an aggressive practice to carry out persistent unsolicited phone calls, emails or any other electronic means, unless this is deemed necessary and justifiable in order to seek fulfilment of legal obligations.

9.3 Do the restrictions noted above apply to marketing sent from other jurisdictions?

Yes, they do.

9.4 Is/are the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?

Yes, they are.

9.5 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?

Due regard shall be paid to the legal basis of the processing and the duty of information (Art. 13 of the GDPR and Art. 14 of the GDPR). Further, the purchaser must be able to demonstrate that it complies with the GDPR and, specifically, that the use of a purchased marketing list complies with any of the legitimate basis of processing as established by Art. 6 of the GDPR. The general rules on sending marketing communications apply.

9.6 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?

The sending of marketing communications in breach of the LSSI shall be punished with a fine of up to EUR 150,000. However, if doing so involved an infringement of the data protection legislation at the same time, then the GDPR administrative fines regime shall be imposed.

10 Cookies

10.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).

The LSSI implements Art. 5 of the EU ePrivacy Directive. Pursuant to Art. 5 of the EU ePrivacy Directive, the storage of cookies (or other data) on an end user’s device requires prior consent (the applicable standard of consent is derived from Directive 95/46/EC and, from 25 May 2018, the GDPR). For consent to be valid, it must be informed, specific, freely given and must constitute a real indication of the individual’s wishes. This does not apply if: (i) the cookie is for the sole purpose of carrying out the transmission of a communication over an electronic communications network; or (ii) the cookie is strictly necessary to provide an “information society
service” (e.g., a service over the internet) requested by the subscriber or user, which means that it must be essential to fulfill their request. The Spanish DPA has published a Guide on Cookies available in Spanish.

10.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?

See the previous answer.

10.3 To date, has/have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?

Yes. For example, a fine was imposed in 2017 on an association that was using the Mailchimp Service in breach of Art. 22.2 of the LSSI. For other sanction resolutions, please visit the Spanish DPA’s website: https://www.aepd.es/resoluciones/.

10.4 What are the maximum penalties for breaches of applicable cookie restrictions?

Failure to provide proper cookie information might lead to fines of up to EUR 30,000 according to the LSSI. If this action is repeated within three years after the first final decision of the Spanish DPA, this might attract fines from EUR 30,000 to EUR 150,000 according to the LSSI.

11 Restrictions on International Data Transfers

11.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.

Data transfers to other jurisdictions that are not within the European Economic Area (the “EEA”) can only take place if the transfer is to an “Adequate Jurisdiction” (as specified by the EU Commission) or the business has implemented one of the required safeguards as specified by the GDPR.

11.2 Please describe the mechanisms businesses typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).

When transferring personal data to a country other than an Adequate Jurisdiction, businesses must ensure that there are appropriate safeguards on the data transfer, as prescribed by the GDPR. The GDPR offers a number of ways to ensure compliance for international data transfers, of which one is consent of the relevant data subject. Other common options are the use of Standard Contractual Clauses or Binding Corporate Rules (“BCRs”). Businesses can adopt the Standard Contractual Clauses drafted by the EU Commission – these are available for transfers between controllers, and transfers between a controller (as exporter) and a processor (as importer). International data transfers may also take place on the basis of contracts agreed between the data exporter and data importer provided that they conform to the protections outlined in the GDPR, and they have prior approval by the relevant data protection authority.

International data transfers within a group of businesses can be safeguarded by the implementation of BCR. The BCRs will always need approval from the relevant data protection authority. Most importantly, the BCRs will need to include a mechanism to ensure they are legally binding and enforced by every member in the group of businesses. Among other things, the BCRs must set out the group structure of the businesses, the proposed data transfers and their purpose, the rights of data subjects, the mechanisms that will be implemented to ensure compliance with the GDPR and the relevant complainant procedures.

Transfer of personal data to the USA is also possible if the data importer has signed up to the EU-US Privacy Shield Framework, which was designed by the US Department of Commerce and the EU Commission to provide businesses in the EU and the US with a mechanism to comply with data protection requirement when transferring personal data from the EU to the US.

11.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.

It is likely that the international data transfer will require prior approval from the relevant data protection authority unless they have already established a GDPR-compliant mechanism, as set out above, for such transfers.

In any case, most of the safeguards outlined in the GDPR will need initial approval from the data protection authority, such as the establishment of BCRs.

According to Article 42 of Spanish Law 3/2018, the following transfers require prior approval of the relevant data protection authority:

- Contractual clauses which have not been approved/adopted by the European Commission.
- Provisions to be inserted into administrative arrangements between public authorities or bodies, which include enforceable and effective data subject rights.

Please note that Spanish Law 3/2018 states that the procedure shall take a maximum of six months.

According to Article 43 of Spanish Law 3/2018, international data transfer based on compelling legitimate interests requires prior notification to the relevant data protection authority.

12 Whistle-blower Hotlines

12.1 What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?

Internal whistle-blowing schemes are generally established pursuant to a concern to implement proper corporate governance principles in the daily functioning of businesses. Whistle-blowing is designed as an additional mechanism for employees to report misconduct internally through a specific channel and supplements a business’ regular information and reporting channels, such as
employee representatives, line management, quality-control personnel or internal auditors who are employed precisely to report such misconducts.

The WP29 has limited its Opinion 1/2006 on the application of EU data protection rules to internal whistle-blowing schemes to the fields of accounting, internal accounting controls, auditing matters, the fight against bribery, banking and financial crime. The scope of corporate whistle-blower hotlines, however, does not need to be limited to any particular issues. In the Opinion, it is recommended that the business responsible for the whistle-blowing scheme should carefully assess whether it might be appropriate to limit the number of persons eligible for reporting alleged misconduct through the whistle-blowing scheme and whether it might be appropriate to limit the number of persons who may be reported through the scheme, in particular in the light of the seriousness of the alleged offences reported.

12.2 Is anonymous reporting prohibited, strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do businesses typically address this issue?

Anonymous reporting is not prohibited under EU data protection law; however, it raises problems as regards the essential requirement that personal data should only be collected fairly. In Opinion 1/2006, the WP29 considered that only identified reports should be advertised in order to satisfy this requirement. Businesses should not encourage or advertise the fact that anonymous reports may be made through a whistle-blower scheme.

An individual who intends to report to a whistle-blowing system should be aware that he/she will not suffer due to his/her action. The whistle-blower, at the time of establishing the first contact with the scheme, should be informed that his/her identity will be kept confidential at all the stages of the process, and in particular will not be disclosed to third parties, such as the incriminated person or to the employee’s line management. If, despite this information, the person reporting to the scheme still wants to remain anonymous, the report will be accepted into the scheme. Whistle-blowers should be informed that their identity may need to be disclosed to the relevant people involved in any further investigation or subsequent judicial proceedings instigated as a result of any enquiry conducted by the whistle-blowing scheme.

According to Article 24 of Spanish Law 3/2018, there could be recorded places of rest, etc. A data protection impact assessment (“DPIA”) must be undertaken with assistance from the Data Protection Officer when there is a systematic monitoring of a publicly accessible area on a large scale. If the DPIA suggests that the processing would result in a high risk to the rights and freedoms of individuals prior to any action being taken by the controller, the controller must consult the data protection authority.

During the course of a consultation, the controller must provide information on the responsibilities of the controller and/or processors involved, the purpose of the intended processing, a copy of the DPIA, the safeguards provided by the GDPR to protect the rights and freedoms of data subjects and where applicable, the contact details of the Data Protection Officer.

If the data protection authority is of the opinion that the CCTV monitoring would infringe the GDPR, it has to provide written advice to the controller within eight weeks of the request of a consultation and can use any of its wider investigative, advisory and corrective powers outlined in the GDPR.

13.2 Are there limits on the purposes for which CCTV data may be used?

The AEPD has published a Guide on the use of CCTV for security and other purposes. It is available here (Spanish): https://www.aepd.es/media/guias/guia-videovigilancia.pdf.

14 Employee Monitoring

14.1 What types of employee monitoring are permitted (if any), and in what circumstances?

Employee monitoring is permitted to control compliance with labour obligations or to ensure the integrity of devices used in the employment.

Monitoring must be lawful, transparent, proportionate and legitimate and there should not be other less intrusive means to reach equivalent goals.

Please note that the WP29 updated its opinion on data processing at work in 2017 (Opinion 2/2017) and that the AEPD is expected to update its guide on data protection in the employment context in 2019.

14.2 Is consent or notice required? Describe how employers typically obtain consent or provide notice.

Consent of employees would not be needed, as notice is required, since control measures on employees are permitted by law (Art. 20.3 of Estatuto de los trabajadores), provided that such control measures comply with the above-mentioned principles.

14.3 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?

Workers’ representatives must generally be informed and in some cases they must also participate in the preparation of documentation (for example, rules on the use of corporate IT tools).
15 Data Security and Data Breach

15.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?

Yes. Personal data must be processed in a way which ensures security and safeguards against unauthorised or unlawful processing, accidental loss, destruction and damage of the data. Both controllers and processors must ensure they have appropriate technical and organisational measures to meet the requirements of the GDPR. Depending on the security risk this may include the encryption of personal data, the ability to ensure the ongoing confidentiality, integrity and resilience of processing systems, an ability to restore access to data following a technical or physical incident and a process for regularly testing and evaluating the technical and organisational measures for ensuring the security of processing.

15.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

The controller is responsible for reporting a personal data breach without undue delay (and in any case within 72 hours of first becoming aware of the breach) to the relevant data protection authority, unless the breach is unlikely to result in a risk to the rights and freedoms of the data subject(s). A processor must notify any data breach to the controller without undue delay.

The notification must include the nature of the personal data breach including the categories and number of data subjects concerned, the name and contact details of the Data Protection Officer or relevant point of contact, the likely consequences of the breach and the measures taken to address the breach including attempts to mitigate possible adverse effects.

15.3 Is there a legal requirement to report data breaches to affected data subjects? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

Controllers have a legal requirement to communicate the breach to the data subject, without undue delay, if the breach is likely to result in a high risk to the rights and freedoms of the data subject.

The notification must include the name and contact details of the Data Protection Officer (or point of contact), the likely consequences of the breach and any measures taken to remedy or mitigate the breach.

The controller may be exempt from notifying the data subject if the risk of harm is remote (e.g., because the affected data is encrypted), the controller has taken measures to minimise the risk of harm (e.g., suspending affected accounts) or the notification requires a disproportionate effort (e.g., a public notice of the breach).

15.4 What are the maximum penalties for data security breaches?

Infringement of data security is subject to administrative fines up to EUR 10 million or 2% of worldwide turnover of the preceding financial year, whichever is higher.

Please note that Spanish Law 3/2018 considers that failure to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, as is required by Art. 32.1 of the GDPR, is a serious infringement.

16 Enforcement and Sanctions

16.1 Describe the enforcement powers of the data protection authority(ies).

<table>
<thead>
<tr>
<th>Investigatory Power</th>
<th>Civil/Administrative Sanction</th>
<th>Criminal Sanction</th>
</tr>
</thead>
<tbody>
<tr>
<td>Investigative Powers</td>
<td>The data protection authority has wide powers to order the controller and the processor to provide any information it requires for the performance of its tasks, to conduct investigations in the form of data protection audits, to carry out review on certificates issued pursuant to the GDPR, to notify the controller or processor of alleged infringement of the GDPR, to access all personal data and all information necessary for the performance of controllers’ or processors’ tasks and access to the premises of the data including any data processing equipment.</td>
<td>N/A</td>
</tr>
<tr>
<td>Corrective Powers</td>
<td>The data protection authority has a wide range of powers including to issue warnings or reprimands for non-compliance, to order the controller to disclose a personal data breach to the data subject, to impose a permanent or temporary ban on processing, to withdraw a certification and to impose an administrative fine (as below).</td>
<td>N/A</td>
</tr>
<tr>
<td>Authorisation and Advisory Powers</td>
<td>The data protection authority has a wide range of powers to advise the controller, accredit certification bodies and to authorise certificates, contractual clauses, administrative arrangements and binding corporate rules as outlined in the GDPR.</td>
<td>N/A</td>
</tr>
<tr>
<td>Imposition of administrative fines for infringements of specified GDPR provisions</td>
<td>The GDPR provides for administrative fines which can be EUR 20 million or up to 4% of the business’ worldwide annual turnover of the proceeding financial year, whichever is higher.</td>
<td>N/A</td>
</tr>
<tr>
<td>Non-compliance with a data protection authority</td>
<td>The GDPR provides for administrative fines which can be EUR 20 million or up to 4% of the business’ worldwide annual turnover of the proceeding financial year, whichever is higher.</td>
<td>N/A</td>
</tr>
</tbody>
</table>
16.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?

The GDPR entitles the relevant data protection authority to impose a temporary or definitive limitation including a ban on processing.

16.3 Describe the data protection authority's approach to exercising those powers, with examples of recent cases.

The AEPD makes its decisions available to the public. Therefore, there are countless enforcement examples available on the AEPD’s website.

16.4 Does the data protection authority ever exercise its powers against businesses established in other jurisdictions? If so, how is this enforced?

Yes. In recent years, the AEPD imposed fines on Facebook, Inc. and Whatsapp, Inc. (see Resolution R/00259/2018). The preliminary questions revolved around the applicable law (please note that this resolution was analysed under the former Spanish Data Protection Law).

17 E-discovery / Disclosure to Foreign Law Enforcement Agencies

17.1 How do businesses typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?

Businesses will typically analyse the request on a case-by-case basis and take into account data protection, labour, criminal and other relevant laws. They will check, among others, if the request was correctly made, if it complies with the legal formalities between the countries, the scope of the request, the legal basis for the disclosure and any international data transfer issues.

17.2 What guidance has/have the data protection authority(ies) issued?

The AEPD analysed the issue in 2011 and published a legal report which was available on its website (see AEPD Report 2011-0469).

18 Trends and Developments

18.1 What enforcement trends have emerged during the previous 12 months? Describe any relevant case law.

There is no relevant sanction procedure resolution of the AEPD addressing the GDPR.

18.2 What “hot topics” are currently a focus for the data protection regulator?

The “hot topics” are the new Spanish Data Protection Law, and the expected updates of various guides (i.e. Guide on Cookies, Guide on data processing in the employment context, etc.).

Further, the AEPD is working on a Circular on data processing by political parties of political opinions. A public consultation has been launched on the draft Circular.
Partner and Head of Information Technology at ECIJA.

With a professional background of more than 20 years in advising leading Spanish and international companies on matters related to information technology, telecommunications, intellectual property, privacy law and compliance regulations, Carlos Pérez Sanz developed most of his career in Landwell – PwC Tax & Legal Services, which he joined in 1998. At PwC, he was a partner and the Head of the Information Technology Department in Spain. Carlos Pérez Sanz holds an LL.B. from Universidad de Barcelona, an M.B.A. from ESADE in Barcelona, and is an associated professor at the same university for its Intellectual Property and Information Society Master’s programme. In addition, he holds the International CISA Certification as a qualified information technology systems’ auditor from ISACA (Information Systems Audit and Control Association).

Carlos Pérez Sanz has played an active role during his professional career in the elaboration process of numerous regulations related to new technology law; in particular, related to the Spanish Data Protection Act, Intellectual Property Act and Information Society Act. He has been selected as one of the best lawyers in information technology and data protection law in Spain by the prestigious international rankings The Legal 500 and Best Lawyers International.

Pia Lestrade Dahms holds a Master’s Degree in Intellectual Property and Information Technology from Spain, as well as a Bachelor of Arts and Juris Doctor from the United States. She works at Ecija Law & Technology on international data protection projects, and serves as the Barcelona Office IP/IT/Privacy Knowledge Professional. She is also the Knowledge Liaison with the law firm’s other offices.

Prior to joining Ecija Law & Technology, Pia interned at Allen & Overy, Chaumet International (LVMH Group), and the U.S. Department of Justice (EOIR Immigration Court).

She has volunteered at technology-related conferences organised by the French Member of Parliament who represented French citizens living in North America. Currently, she acts as the Young Privacy Professional Leader to the Barcelona Chapter of the International Association of Privacy Professionals (IAPP).
Chapter 41

Sweden

Bird & Bird

Mattias Lindberg  Marcus Lorentzon

1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

The EU Regulation (EU) 2016/679 (the “General Data Protection Regulation” or “GDPR”) is the principal data protection legislation in the EU, hence also in Sweden. Under the GDPR, the data protection legislation across the EU Member States is harmonised, though not totally, since there are a lot of other data protection acts that still will be in force (e.g. covering areas such as healthcare and financial activities).

As a result of the GDPR, a new Data Protection Act (“DPA”) have entered into force in Sweden. The new DPA will complement the GDPR in regard to the areas in which the GDPR opens up for national legislation.

1.2 Is there any other general legislation that impacts data protection?

The ePrivacy Directive 2002/58/EC is implemented into Swedish legislation through a number of laws, e.g. the Electronic Communications Act. The European Convention on Human Rights has been incorporated into Swedish law which, primarily for the purpose of data protection, has an impact on the Swedish principle of openness (Sw. offentlighetsprincipen) and freedom of the press and freedom of speech (Sw. tryck- och yttrandefriheten).


The EU Commission has proposed a new regulation on privacy and electronic communications that will apply to telecom and internet operators and replace the current Directive. The ePrivacy Regulation (“the ePR”) would harmonise the applicable rules across the EU. The ePR is still a draft at this stage and it is unclear when it will be finalised, what it will contain and when it will enter into force.

The DPA authorises the government and the Swedish data protection authority, the Data Inspection Board (“DIB”), to issue more detailed regulations concerning several features of the DPA.

1.3 Is there any sector-specific legislation that impacts data protection?

There are hundreds of acts and ordinances containing regulations for registration and Processing of Personal Data, covering areas such as healthcare and financial activities.

1.4 What authority(ies) are responsible for data protection?

According to the GDPR, it is mandatory for each EU Member State to provide for one or more supervisory authority/authorities to be responsible for monitoring the application of the GDPR. In Sweden, the Swedish data protection authority, the DIB, is responsible for the monitoring of the data protection legislation.

The DIB ensures that authorities, companies, organisations and individuals follow (i) the GDPR, (ii) the Data Protection Act, (iii) the Camera Surveillance Act, (iv) the Debt Recovery Act, and (v) the Credit Information Act.

Furthermore, The DIB works to prevent intrusion upon privacy through information and by issuing directives and codes of statutes. The DIB also handles complaints, regarding the data protection legislation, from individuals and organisations and carries out inspections. Inspections may be triggered by complaints but are normally planned and conducted in campaigns for sector-specific areas.

The DIB is a part of the European Data Protection Board (“EDPB”), which is an independent European authority, which contributes to the consistent application of the GDPR throughout the EU.

The Swedish Post and Telecom Authority (Sw. Post- och telestyrelsen “PTS”) is the supervisory authority regarding the Electronic Communications Act. Thus, PTS monitors the usage of cookies.

2 Definitions

2.1 Please provide the key definitions used in the relevant legislation:

- “Personal Data” means any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online
Do the data protection laws apply to businesses outside the EU?

Yes; since the GDPR harmonises the data protection legislation across the EU Member States, some of the data protection laws apply to businesses outside of Sweden. All businesses that Process Personal Data, either as a Controller or Processor, and that are established in any EU Member State, fall under the scope of the GDPR, regardless of whether or not the Processing takes place in the EU.

Furthermore, the GDPR applies to businesses that are established outside the EU, either if they are subject to the laws of an EU Member State or if they are Processing Personal Data of EU residents to be able offer goods or services or to monitor the behaviour of EU residents (if such behaviour takes place in the EU).

4 Key Principles

4.1 What are the key principles that apply to the processing of personal data?

Transparency

Personal Data must be Processed lawfully, fairly and in a transparent manner in relation to the Data Subject. This means that the Controller must provide the Data Subject with certain minimum information, provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language, regarding the collection and Processing of the Personal Data.

LAWful basis for processing

It is only lawful to Process Personal Data to the extent it is permitted under the applicable data protection laws. According to the GDPR, Processing of Personal Data is permitted if: (i) the Data Subject has given Consent to the Processing of his or her Personal Data for one or more specific purposes; (ii) Processing is necessary for the performance of a contract to which the Data Subject is party or in order to take steps at the request of the Data Subject prior to entering into a contract; (iii) Processing is necessary for compliance with a legal obligation to which the Controller is subject; (iv) Processing is necessary in order to protect the vital interests of the Data Subject or of another natural person; (v) Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Controller; or (vi) Processing is necessary for the purposes of the legitimate interests pursued by the Controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the Data Subject which require protection of Personal Data, in particular where the Data Subject is a child.

Processing of Sensitive Personal Data, such as data concerning health, political opinion or religious beliefs, is only lawful under certain conditions and requires stronger legal grounds than regular Personal Data.

Purpose limitation

Personal Data may only be collected for specified, explicit and legitimate purposes and must not be further Processed in a manner that is incompatible with those purposes. In certain cases, a Controller may use the relevant Personal Data in a manner that is incompatible with the purposes for which they were initially collected.

Data minimisation

Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which those data are Processed.

Proportionality

Proportionality is a general principle both within the EU law and in Swedish substantive law. In regard to the GDPR, proportionality means that Processing activities, safeguards and other measures that are prescribed by the GDPR should not go beyond what is necessary for the purpose in question.

Retention

Personal Data must be kept in a form that permits identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data are Processed.

Other key principles – please specify

Accuracy

Personal Data must be accurate and, where necessary, kept up to date; hence the Controller must take every reasonable step to ensure that Personal Data that are inaccurate are either erased or rectified without delay.
5 Individual Rights

5.1 What are the key rights that individuals have in relation to the processing of their personal data?

- **Data security**
  Personal Data must be Processed in a manner that ensures appropriate security of those data, including protection against unauthorised or unlawful Processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

- **Accountability**
  The Controller is responsible for, and must be able to demonstrate, compliance with the data protection principles set out above.

- **Right of access to data/copies of data**
  A Data Subject has the right to obtain from a Controller the following information in respect of the Data Subject’s Personal Data: (i) confirmation of whether, and where, the Controller is Processing the Data Subject’s Personal Data; (ii) information about the purposes of the Processing; (iii) information about the categories of Personal Data being Processed; (iv) information about the categories of recipients with whom the Personal Data may be shared; (v) information about the period for which the Personal Data will be stored (or the criteria used to be determine that period); (vi) information about the existence of the rights to erasure, to rectification, to restrict Processing and to object to Processing; (vii) information about the existence of the right to complain to the relevant data protection authority; (viii) where the data were not collected from the Data Subject, information as to the source of the Personal Data; and (ix) information about the existence of, and an explanation of the logic involved in, any automated Processing that has a significant effect on the Data Subject.

- **Right to rectification of errors**
  Controllers must ensure that inaccurate or incomplete data are erased or rectified. Data Subjects have the right to rectification of inaccurate Personal Data.

- **Right to deletion/right to be forgotten**
  The right to be forgotten is probably one of the most well-known rights in the GDPR. However, the right to be forgotten is not an absolute right, as the name may suggest. The right to be forgotten means that the Data Subjects have the right to erasure of their Personal Data if: (i) the data are no longer needed for their original purpose (and no new lawful purpose exists); (ii) the lawful basis for the Processing is the Data Subject’s Consent, the Data Subject withdraws that Consent and no other lawful ground exists; (iii) the Data Subject exercises the right to object, and the Controller has no overriding grounds for continuing the Processing; (iv) the Personal Data have been Processed unlawfully; or (v) erasure is necessary for compliance with EU law or national data protection law.

- **Right to object to processing**
  Data Subjects have the right to object, on grounds relating to their particular situation, to the Processing of Personal Data where the basis for that Processing is either public interest or legitimate interest of the Controller. The Controller must cease such Processing unless it demonstrates compelling legitimate grounds for the Processing which override the interests, rights and freedoms of the relevant Data Subject or requires the Personal Data in order to establish, exercise or defend legal rights.

- **Right to restrict processing**
  Data Subjects have the right to restrict the Processing of Personal Data, which means that the Personal Data may only be held by the Controller, and may only be used for limited purposes if: (i) the accuracy of the Personal Data is contested (and only for as long as it takes to verify that accuracy); (ii) the Processing is unlawful and the Data Subject requests restriction (as opposed to exercising the right to erasure); (iii) the Controller no longer needs the Personal Data for their original purpose, but the data are still required by the Controller to establish, exercise or defend legal rights; or (iv) verification of overriding grounds is pending, in the context of an erasure request.

- **Right to data portability**
  Data Subjects have a right to receive a copy of their Personal Data in a commonly used machine-readable format and transfer their Personal Data from one Controller to another or have the data transmitted directly between Controllers.

- **Right to withdraw consent**
  Data Subjects have the right to withdraw their Consent at any time. The withdrawal of Consent does not affect the lawfulness of Processing based on Consent before its withdrawal. Prior to giving Consent, the Data Subject must be informed of the right to withdraw Consent. It must be easy to withdraw Consent as to give it.

- **Right to object to marketing**
  Data Subjects have the right to object to the Processing of Personal Data for the purpose of direct marketing, including profiling.

- **Right to complain to the relevant data protection authority(ies)**
  Data Subjects have the right to lodge complaints concerning the Processing of their Personal Data with the DIB, if the Data Subject lives in Sweden or the alleged infringement occurred in Sweden.

  Other key rights – please specify

- **Right not to be subject to a decision based solely on automated processing**
  The Data Subject has the right not to be subject to a decision based solely on automated Processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

- **Right to basic information**
  Data Subjects have the right to be provided with information on the identity of the Controller, the reasons for Processing their Personal Data and other relevant information necessary to ensure the fair and transparent Processing of Personal Data.

6 Registration Formalities and Prior Approval

6.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?

The Data Protection Directive 95/46/EC and the old DPA prescribed a general obligation to notify Processing of Personal Data to the DIB. This obligation led to an administrative and financial burden but did not always improve personal protection. Therefore, the GDPR does not contain any such obligations. Instead of the general obligation to notify the supervisory authority, the GDPR prescribes that the Controller shall perform a data protection impact assessment (“DPIA”) or a prior consultation with the supervisory authority if the
Processing is likely to, or would, result in a high risk to the rights and freedoms of natural persons. The supervisory authority shall establish and make public a list of the kind of Processing operations which are subject to the requirement for a DPIA.

6.2 If such registration/notification is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?

This is not applicable in Sweden.

6.3 On what basis are registrations/notifications made (e.g., per legal entity, per processing purpose, per data category, per system or database)?

This is not applicable in Sweden.

6.4 Who must register with/notify the data protection authority (e.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation)?

This is not applicable in Sweden.

6.5 What information must be included in the registration/notification (e.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes)?

This is not applicable in Sweden.

6.6 What are the sanctions for failure to register/notify where required?

This is not applicable in Sweden.

6.7 What is the fee per registration/notification (if applicable)?

This is not applicable in Sweden.

6.8 How frequently must registrations/notifications be renewed (if applicable)?

This is not applicable in Sweden.

6.9 Is any prior approval required from the data protection regulator?

There is no such requirement in Sweden.

6.10 Can the registration/notification be completed online?

This is not applicable in Sweden.

6.11 Is there a publicly available list of completed registrations/notifications?

There is no such list.

6.12 How long does a typical registration/notification process take?

This is not applicable in Sweden.

7 Appointment of a Data Protection Officer

7.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.

In some circumstances, it is mandatory for Controllers and the Processors to appoint a Data Protection Officer, the most relevant circumstances being large-scale and systematic monitoring of individuals and/or large-scale Processing of Sensitive Personal Data.

7.2 What are the sanctions for failing to appoint a Data Protection Officer where required?

If the Controller or Processor fail to comply with a mandatory appointment of a Data Protection Officer, the Controller or Processor may be penalised with any penalties available under the GDPR.

7.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect of his or her role as a Data Protection Officer?

The appointed Data Protection Officer should not be dismissed or penalised for performing their tasks and should report directly to the highest management level of the Controller or Processor.

7.4 Can a business appoint a single Data Protection Officer to cover multiple entities?

Yes, provided that the Data Protection Officer is easily accessible from each establishment.

7.5 Please describe any specific qualifications for the Data Protection Officer required by law.

The Data Protection Officer should be appointed on the basis of professional qualities and should have an expert knowledge of data protection law and practices.

7.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?

The GDPR outlines the minimum tasks required by the Data Protection Officer, which include: (i) informing the Controller, Processor and their relevant employees who Process Personal Data of their obligations under the GDPR; (ii) monitoring compliance with the GDPR, national data protection legislation and internal policies in relation to the Processing of Personal Data including internal audits; (iii) advising on DPIAs and the training of staff; and (iv) co-operating with the data protection authority and acting as the authority’s primary contact point for issues related to Processing of Personal Data.
The Controller or Processor must notify the DIB of the contact details of the Data Protection Officer.

8.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?

The Processor must be appointed under a binding agreement in writing. The contractual terms must stipulate that the Processor: (i) only acts on the documented instructions of the Controller; (ii) imposes confidentiality obligations on all employees; (iii) ensures the security of Personal Data that it Processes; (iv) abides by the rules of regarding the appointment of sub-Processors; (v) implements measures to assist the Controller with guaranteeing the rights of Data Subjects; (vi) assists the Controller in obtaining approval from the Data Protection Officer; (vii) either returns or destroys the Personal Data at the end of the relationship (except as required by EU or Member State law); and (viii) provides the Controller with all the information necessary to demonstrate compliance with the GDPR.

9.1 Please describe any legislative restrictions on the sending of electronic direct marketing (e.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?).

The Marketing Act has regulations on marketing by email, fax or telephone. Under the Marketing Act, a trader may, in the course of marketing to a natural person, use email, a telex or automatic calling device or any other similar automatic system for individual communication that is not operated by an individual, only if the natural person has Consented to this in advance. Where a trader has obtained details of a natural person’s email address in the context of a sale of a product to that person, the Consent requirement shall not apply, provided that (i) the natural person has not objected to the use of the email address for the purpose of marketing via email, (ii) the marketing relates to the trader’s own similar products, and (iii) the natural person is clearly and explicitly given the opportunity to object, simply and without charge, to the use of such details for marketing purposes, when they are collected and in conjunction with each subsequent marketing communication.

Regarding marketing via email, the communication shall, at all times, contain a valid address to which the recipient can send a request that the marketing cease. This also applies to marketing to a legal person.

According to the GDPR, the Data Subject shall have the right to object at any time to Processing of Personal Data concerning him or her for direct marketing purposes, which includes profiling to the extent that it is related to such direct marketing. Where the Data Subject objects to Processing for direct marketing purposes, the Personal Data shall no longer be Processed for such purposes.

9.2 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.).

The Marketing Act prescribes that traders may use means of distance communication other than, for example, SMS and email, for marketing purposes unless the natural person clearly opposes the use of the method.

Good marketing practice requires marketers – before a call is made to a consumer for sales, marketing or fundraising purposes – to control if the consumer’s phone number is in the blocking registry (NIX-Telefon). The blocking registry is an opt-out registry which includes, from the year 2015, both regular phones and mobile phones. If a control is made, the company is entitled to call the consumer within two months from the day on which the used version of the track log was updated.

Since the rules regarding direct marketing in the Marketing Act originate from Directive 2009/136/EC, which will be replaced by the ePR, the legislation might be changed when the ePR enters into force. However, due to disagreements within the negotiations regarding the ePR, one can only speculate about the content in the final draft.

9.3 Do the restrictions noted above apply to marketing sent from other jurisdictions?

Yes, the Marketing Act applies to foreign companies provided that they target the marketing to a Swedish audience.

9.4 Is/are the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?

Yes, it is.

9.5 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?

Yes, it is lawful. Marketers need to follow good marketing practice, which includes sector-specific ethical rules.
Breaches of the restrictions in the Marketing Act may result in a penalty. In recent years, a standard of 5,000,000 Swedish kronor has been used. In addition, both traders and natural persons may claim damages.

Furthermore, traders may be ordered to pay a special charge (market disruption charge) if the trader, or a person acting on behalf of the trader, intentionally or negligently contravenes obligations in the Marketing Act. The market disruption charge shall be no less than 5,000 Swedish kronor and no more than 5,000,000 Swedish kronor. However, the charge may not exceed 10% of the trader’s annual turnover.

9.6 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?

No such final assessments have been rendered yet. Hence, the preliminary standpoints are not binding but may nevertheless be indicative for companies who must observe the regulations on Consent in the Electronic Communications Act.

10.4 What are the maximum penalties for breaches of applicable cookie restrictions?

The penalty for breaches is a fine. The amount varies depending on the circumstances.

10 Cookies

10.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).

The Electronic Communications Act states that information may be stored in or retrieved from a subscriber’s or user’s terminal equipment only if subscribers or users are provided with access to information on the purpose of the Processing and Consents to the Processing. For Consent to be valid, it must be informed, specific, freely given and must constitute a real indication of the individual’s wishes.

This does not apply to the storage or retrieval necessary for the transmission of an electronic message over an electronic communications network, or for the provision of a service explicitly requested by the subscriber or user.

Since the rules regarding cookies in the Electronic Communications Act originate from Directive 2009/136/EC, which will be replaced by the ePR, the legislation might be changed when the ePR enters into force. However, due to disagreements within the negotiations regarding the ePR, one can only speculate about the content in the final draft.

10.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?

The Electronic Communications Act does not make any distinction between different types of cookies.

10.3 To date, has/have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?

Yes, the PTS has carried out supervision in respect of the Processing of data and obtaining Consent in relation to cookies. The supervisions include how the companies obtain their respective Consent to use cookies. The PTS has thereafter produced a preliminary assessment based upon those supervisions on obtaining Consent in its endeavour for the general public to have greater insights and more influence over how personal information is used in connection with the use of telephones and the internet. A final assessment from the PTS will only be available in the respective decisions in regard to the supervisions of the respective companies.

In principle, data transfers to jurisdictions outside of the EU and/or the European Economic Area (the “EEA”) are not permitted. Data transfers to a jurisdiction outside the EU/EEA can only take place if the Data Subject Consents to the transfer, if transfer is to an “Adequate Jurisdiction”, if the business has implemented one of the derogations specified in the GDPR applies to the relevant transfer.

11 Restrictions on International Data Transfers

11.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.

When transferring Personal Data to a country other than an Adequate Jurisdiction, businesses must ensure that there are appropriate safeguards on the data transfer, as prescribed by the GDPR.

For smaller businesses, the easiest way to comply with the data transfer rules is to get the Consent of the Data Subject or to carry out the data transfer as a result of the performance of a contract with the Data Subject.

For international businesses, data transfer to a jurisdiction outside of the EU/EEA can be safeguarded by the implementation of Binding Corporate Rules (“BCRs”). The BCRs will always need approval from the relevant data protection authority.

Furthermore, businesses can adopt the Standard Contractual Clauses drafted by the EU Commission. The Standard Contractual Clauses are available for transfers between Controllers, and transfers between a Controller and a Processor.

Transfer of Personal Data to the US is also possible under the EU-US Privacy Shield Framework.

11.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.

Most of the safeguards outlined in the GDPR will need initial approval from the DIB.
12 Whistle-blower Hotlines

12.1 What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?

Whistle-blowing hotlines are generally established in order to implement proper corporate governance principles in the daily functioning of businesses. However, the Controller must comply with the fundamental requirements of the GDPR, and therefore have a legal ground; for example, for the Processing and provision of sufficient information to the Data Subjects. Furthermore, the DIB prescribes that the Controller must perform a DPIA prior to the whistle-blower hotline being set up.

The WP29 (the predecessor to the EDPB) recommended that the business responsible for the whistle-blowing scheme should carefully assess whether it might be appropriate to limit the number of persons eligible for reporting alleged misconduct through the whistle-blowing scheme and whether it might be appropriate to limit the number of persons who may be reported through the scheme; in particular, in the light of the seriousness of the alleged offences reported.

12.2 Is anonymous reporting prohibited, strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do businesses typically address this issue?

As there is no specific statute or guidance, anonymous reporting is not strictly prohibited or strongly discouraged under EU data protection law.

The whistle-blower, at the time of establishing the first contact with the scheme, should be informed that his/her identity will be kept confidential at all stages of the process, and in particular will not be disclosed to third parties, such as the incriminated person or the employee’s line management. If, despite this information, the person reporting to the scheme still wants to remain anonymous, the report will be accepted.

13 CCTV

13.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?

A new Camera Surveillance Act entered into force August 1, 2018. The Camera Surveillance Act regulates the use of equipment for audio-visual monitoring and surveillance. In general, the Camera Surveillance Act prescribes that private businesses do not need to apply for a permit in order to use CCTV. Authorities and other entities who perform tasks of general interest need a permit to use CCTV. However, all entities must ensure that the usage of CCTV complies with the rules in the GDPR.

The Camera Surveillance Act prescribes quite extensive requirements regarding informing the Data Subjects about the usage of CCTV. In the proximity of a CCTV camera, a sign that provides the Data Subject with information must be put up. The information should include information on the identity and contact information of the Controller. Further information should be posted on the Controller’s website.

From the data privacy perspective, a DPIA must usually be undertaken with assistance from the Data Protection Officer, especially if the CCTV is systematically monitoring a publicly accessible area on a large scale. If the DPIA suggests that the Processing would result in a high risk to the rights and freedoms of individuals prior to any action being taken by the Controller, the Controller must consult the DIB.

13.2 Are there limits on the purposes for which CCTV data may be used?

According to the Camera Surveillance Act, permission for CCTV shall be given if the Controllers interest in such surveillance weighs heavier than the Data Subjects’ interest in not being surveilled. When performing the interest assessment, special attention should be paid to whether the surveillance is needed to prevent, investigate and reveal crimes, prevent accidents and other comparable purposes.

14 Employee Monitoring

14.1 What types of employee monitoring are permitted (if any), and in what circumstances?

Employee monitoring is subject to the general requirements of the GDPR. However, in the opinion of the DIB, employers cannot rely on Consent from employees to the Processing of Personal Data that occurs when an employee monitoring system is used. This is because employees often find themselves in a position of dependence upon their employers and are therefore unable to give the voluntary Consent required by the GDPR.

It has become more and more common for employers to use positioning systems of various kinds to check where their employees are.

14.2 Is consent or notice required? Describe how employers typically obtain consent or provide notice.

Employers typically obtain Consent either by the employment agreement or by referencing the company’s Privacy Policy. The employer can also justify its actions by a balance of interests in accordance with the GDPR.

It should be noted that in the opinion of the DIB, employers cannot rely on Consent from employees to the Processing of Personal Data. This is because employees often find themselves in a position of dependence upon their employers and are therefore unable to give the voluntary Consent demanded by the GDPR. Employers who want to use employee monitoring must normally rely on a balance of interests. The employer’s interest in carrying out the Processing must then outweigh the employee’s interest in protection from an invasion of privacy. In the overall assessment that must be performed in these cases, the following factors must be considered:

(i) the purpose of the Processing; (ii) how the data are handled and how the results are used; (iii) what information is given to the employees; (iv) whether the Processing can be performed in a way that involves less invasion of privacy; (v) what technical and administrative security is available for the data; (vi) the existence of collective agreements and the content of these; and (vii) whether the Processing follows good practice for the labour market.
14.3 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?

There is no absolute requirement to receive an approval from the relevant trade union. However, in the balance of interests in accordance with the GDPR, the opinion of the trade union may become an important factor. It is therefore important for the employer (and the Data Protection Officer) to have a good and productive relationship with the trade unions in the discussions of whether the Processing follows good practice for the labour market or not. Hence, it is normally well-invested time to initiate a discussion with the relevant trade union at an early stage in the process.

15 Data Security and Data Breach

15.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?

Yes, the Controller and Processor must ensure they have appropriate technical and organisational measures in place to meet the requirements of the GDPR. Depending on the security risk, this may include (i) the encryption of Personal Data, (ii) the ability to ensure the ongoing confidentiality, integrity and resilience of Processing systems, (iii) an ability to restore access to data following a technical or physical incident, and (iv) a process for regularly testing and evaluating the technical and organisational measures for ensuring the security of Processing.

15.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

Yes, the Controller is responsible for reporting a Personal Data Breach without undue delay (and in any case within 72 hours of first becoming aware of the breach) to the DIB, unless the breach is unlikely to result in a risk to the rights and freedoms of the Data Subjects. A Processor must notify any Data Breach to the Controller without undue delay, so that the Controller can report the Data Breach to the DIB.

The notification must include (i) the nature of the Personal Data Breach including the categories and number of Data Subjects concerned, (ii) contact details of the Data Protection Officer, (iii) the likely consequences of the breach, and (iv) the measures taken to address the breach including attempts to mitigate possible adverse effects.

15.3 Is there a legal requirement to report data breaches to affected data subjects? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

Controllers have a legal requirement to communicate the breach to the Data Subject, without undue delay, if the breach is likely to result in a high risk to the rights and freedoms of the Data Subject.

The notification must include (i) the contact details of the Data Protection Officer, (ii) the likely consequences of the breach, and (iii) any measures taken to remedy or mitigate the breach.

Under some circumstances, the Controller may be exempt from notifying the Data Subject (e.g. if the risk of harm is remote or if the Controller has taken measures to minimise the risk).

15.4 What are the maximum penalties for data security breaches?

The maximum penalty is the higher of €20 million or 4% of worldwide turnover.

16 Enforcement and Sanctions

16.1 Describe the enforcement powers of the data protection authority(ies).

<table>
<thead>
<tr>
<th>Investigatory Power</th>
<th>Civil/Administrative Sanction</th>
<th>Criminal Sanction</th>
</tr>
</thead>
<tbody>
<tr>
<td>Investigative Powers</td>
<td>The DIB has wide powers to order the Controller and the Processor to provide any information it requires for the performance of its tasks, to conduct investigations in the form of data protection audits, to carry out reviews on certificates issued pursuant to the GDPR, to notify the Controller or Processor of alleged infringement of the GDPR, to access all Personal Data and all information necessary for the performance of Controllers’ or Processors’ tasks and access to the premises of the data including any data Processing equipment.</td>
<td>N/A</td>
</tr>
<tr>
<td>Corrective Powers</td>
<td>The DIB has a wide range of powers including to issue warnings or reprimands for non-compliance, to order the Controller to disclose a Personal Data Breach to the Data Subject, to impose a permanent or temporary ban on Processing, to withdraw a certification and to impose an administrative fine (as below).</td>
<td>N/A</td>
</tr>
<tr>
<td>Authorisation and Advisory Powers</td>
<td>The DIB has a wide range of powers to advise the Controller, accredit certification bodies and to authorise certificates, contractual clauses, administrative arrangements and binding corporate rules as outlined in the GDPR.</td>
<td>N/A</td>
</tr>
<tr>
<td>Imposition of Administrative Fines for Infringements of Specified GDPR Provisions</td>
<td>The GDPR provides for administrative fines which can be €20 million or up to 4% of the business’ worldwide annual turnover of the proceeding financial year.</td>
<td>N/A</td>
</tr>
<tr>
<td>Non-Compliance with a Data Protection Authority</td>
<td>The GDPR provides for administrative fines which will be €20 million or up to 4% of the business’ worldwide annual turnover of the proceeding financial year, whichever is higher.</td>
<td>N/A</td>
</tr>
</tbody>
</table>
18.1 What enforcement trends have emerged during the previous 12 months? Describe any relevant case law.

In Sweden, there is an extreme focus on integrity in both the strategic agreements and within the businesses. This trend is partly because of the new EU regulations, but also due to a large scandal regarding the government’s use of Personal Data and data security, during the summer of 2017.

The Swedish market is placing more and more focus on privacy issues in general by internally improving its processes in regard to quality. The DIB is encouraging entities to build privacy and data protection measures into the design of their data Processing in order to facilitate compliance with privacy and data protection principles. Hence, there is a lot of work going on so that authorities, companies, organisations and individuals will be able to meet the challenges resulting from the GDPR and the use of new technologies.

During March 2019, the DIB adopted a supervisory plan for 2019 and 2020, in which the DIB sets out what industries and what areas of the GDPR will be the focus of the enforcement activities of the DIB. The industries in focus include, among others, healthcare, education and retail. The specific areas of the GDPR include the role as Controller and Processor, Consent and the applicability of the GDPR in relation to other laws that regulate the Processing of Personal Data.

In addition, the DIB has conducted a couple of enforcements that caught the public’s attention, both in response to Data Breaches and in response to complaints from the public.

As of May 2019, no administrative fines have yet been imposed in Sweden. However, the first administrative fines are likely to be imposed in the near future.

18.2 What “hot topics” are currently a focus for the data protection regulator?

In general, the DIB is increasingly placing emphasis on the advice towards companies and organisations to conduct integrity analysis when making important business decisions with regards to privacy issues.

The legislator is working hard to implement the data protection reform and update other registry legislation to function with the GDPR. Furthermore, the legislator has to face the challenges that come along with the digitalisation of society.
Mattias Lindberg is a Partner & Head of Commercial, Sweden at Bird & Bird.

Mattias Lindberg has broad experience in providing legal advice and suggested measures in local and multi-jurisdictional outsourcing, strategic agreements, IT law and privacy law.

As a Data Privacy expert, Mattias Lindberg has extensive experience of analysing and implementing business-critical processes for the handling of personal data. He takes a methodical and pedagogic approach when analysing, optimising and implementing authority-regulated operational processes. As the personal data protection officer for several companies, Mattias Lindberg has extensive experience of implementing operational processes in accordance with the General Data Protection Regulation and the Patient Data Act.

Mattias Lindberg provides advice concerning all aspects of personal data management and regularly produces strategies regarding how personal data should be implemented and handled, and how integrity analysis should be conducted. Mattias Lindberg places particular focus on ensuring that the information is not only handled in accordance with the applicable laws and regulations, but that it is also handled in as practical and cost-effective a manner as possible. In addition, Mattias Lindberg has a great deal of experience in handling both ongoing contacts with the Data Inspection Board and audits conducted by the Board. He is also a highly-regarded public speaker and is regularly invited to speak on various aspects of commercial law.

Marcus Lorentzon is an associate at Bird & Bird.

Marcus Lorentzon has extensive experience within the fields of IT law and privacy law and provides advice concerning all aspects of privacy law. Marcus also holds experience of implementing operational processes in accordance with the General Data Protection Regulation and the Patient Data Act.

Furthermore, Marcus is specialised in tort and insurance law and has for several years worked within the insurance industry. Marcus is used to working with both the legal and commercial risks that companies face in their business and has good knowledge in managing and eliminating such risks.
Chapter 42

Switzerland

Pestalozzi Attorneys at Law

1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

The Federal Act on Data Protection of 19 June 1992 (the Data Protection Act, the “DPA”) and the Ordinance to the Federal Act on Data Protection of 14 June 1993 (“ODPA”).

In March 2019, the Schengen Federal Data Protection Act entered into force. In addition, a total revision of the Data Protection Act is pending.

Since Switzerland is not a member of the EU, it does not have to comply with the EU General Data Protection Regulation or any other directives applicable in this field.

1.2 Is there any other general legislation that impacts data protection?

Every Swiss canton has its own data protection statutes with respect to data processing by cantonal public authorities.

Finally, there are some specific provisions in labour laws regarding monitoring of employees.

1.3 Is there any sector-specific legislation that impacts data protection?

The Swiss banking secrecy and guidelines thereto impact data protection when bank customer data are processed. Furthermore, secrecy obligations, such as patient secrecy regarding health data as set out in article 321 of the Swiss Criminal Code, have an impact on when respective data are processed. Particular rules concerning data retention and processing also apply in the telecommunication sector.

1.4 What authority(ies) are responsible for data protection?

The Federal Data Protection and Information Commissioner (“FDPIC”) is the relevant authority if personal data are processed by federal authorities, individuals and legal entities. The respective Cantonal Data Protection and Information Officer in each canton is the responsible authority if personal data are processed by public authorities of the respective canton.

2 Definitions

2.1 Please provide the key definitions used in the relevant legislation:

■ “Personal Data”

All information relating to an identified or identifiable natural or legal person (see article 3 lit. a and b DPA).

■ “Processing”

Any operation with personal data, irrespective of the means applied and the procedure, and in particular the collection, storage, use, revision, disclosure, archiving or destruction of data (see article 3 lit. e DPA).

■ “Controller”

There is no statutory definition, as the term is not explicitly used in the DPA. The FDPIC defines “Data Controller” or “Data Exporter” in its template outsourcing agreement as follows: the natural or legal person, public authority, agency or any other body established in Switzerland which alone or jointly with others determines the purposes and means of the processing of personal data and which transfers such data (to another country) for the purposes of its processing on his/her behalf.

■ “Processor”

There is no statutory definition, as the term is not explicitly used in the DPA. The FDPIC defines “Data Processor” or “Data Importer” in its template outsourcing agreement as follows: natural or legal person, public authority, agency or any other body (established in another country) which agrees to receive personal data from the Data Exporter for the purposes of processing such data on behalf of the latter after the transfer in accordance with his/her instructions.

■ “Data Subject”

Natural or legal persons whose data are processed (see article 3 lit. b DPA). It is important to emphasise that the DPA does not only protect personal data of natural persons as most other data protection laws, but also personal data of legal persons.

■ “Sensitive Personal Data”

Data on: 1) religious, ideological, political or trade union-related views or activities; 2) health, the intimate sphere or racial origin; 3) social security measures; and 4) administrative or criminal proceedings and sanctions (see article 3 lit. c DPA).

■ “Data Breach”

There is no statutory definition, as the term is not explicitly used in the DPA.

■ “Data Owner”

The term used in the DPA is “Controller of the Data File”,
which is any private person or federal body that decides on the purpose and content of a data file (see article 3 lit. i DPA).

- **“Pseudonymous Data”**
  There is no statutory definition. Pseudonymous data are data for which the relation to a natural or legal person is not entirely removed, but rather replaced by a code, which can be attributed based on a specific rule to the respective natural or legal person. Anonymous data are data for which the relation to a natural or legal person is entirely removed.

- **“Personality Profile”**
  A collection of data that permits an assessment of essential characteristics of the personality of a natural person (see article 3 lit. d DPA).

- **“Data Files”**
  Any set of personal data that is structured in such a way that the data are accessible by the data subject (see article 3 lit. g DPA).

### 3 Territorial Scope

#### 3.1 Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to those laws?

The DPA applies as soon as data are processed in Switzerland. Thus, if personal data are archived in Switzerland (e.g., in the cloud), the DPA will apply – even though no data were collected in Switzerland and the data subjects are not located in Switzerland.

### 4 Key Principles

#### 4.1 What are the key principles that apply to the processing of personal data?

- **Transparency**
  The collection of personal data and in particular the purpose of its processing must be evident to the data subject (see article 4 para. 4 DPA).

- **Lawful basis for processing**
  Personal data may only be processed lawfully (see article 4 para. 1 DPA).

- **Purpose limitation**
  Personal data may only be processed for the purpose indicated at the time of collection, that is evident from the circumstances, or that is provided for by law (see article 4 para. 3 DPA).

- **Data minimisation**
  There is no such principle set out in the DPA, but the FDPIC considers that it is part of the general principle of proportionality.

- **Proportionality**
  Data processing must be carried out in good faith and must be proportionate (see article 4 para. 2 DPA).

- **Retention**
  This is not a key principle set out in the DPA. However, the principle of proportionality requires that personal data are only retained as long as it is necessary with respect to the purpose of the data processing. General data retention requirements are not set forth in the DPA, but rather in the Swiss Code of Obligations or sector-specific regulations.

### 5 Individual Rights

#### 5.1 What are the key rights that individuals have in relation to the processing of their personal data?

- **Right of access to data/copies of data**
  Any person may request information from the Controller of the Data File as to whether data concerning him/her is being processed (see article 8 para. 1 DPA; exceptions are mentioned in article 9 DPA). The information must normally be provided in writing, in the form of a printout or a photocopy, and is free of charge.

- **Right to rectification of errors**
  Any data subject may request that incorrect data be corrected (see article 5 para. 2 DPA).

- **Right to deletion/right to be forgotten**
  Any data subject may request that incorrect data be deleted (see article 5 para. 2 DPA). The right to be forgotten is not explicitly mentioned in the DPA, but the FDPIC and case law consider that such a right results from the general principle of proportionality.

- **Right to object to processing**
  Data subjects may request (in a civil litigation) that data processing be stopped, that no data be disclosed to third parties, or that the personal data be corrected or destroyed (see article 15 para. 1 DPA). It is important to note that data processing may be blocked by preliminary injunctions.

- **Right to restrict processing**
  There is no such principle set out in the DPA.

- **Right to data portability**
  There is no such principle set out in the DPA.

- **Right to withdraw consent**
  According to article 12 para. 2 lit. b DPA, “anyone must not process data pertaining to a person against that person’s express wish without justification”. Based on this provision, it is possible to withdraw consent at any time.

- **Right to object to marketing**
  In addition to the objection to data processing for marketing purposes as set out above, there is a special regulation regarding mass emails (i.e., marketing newsletters) in article 3 lit. o of the Unfair Competition Act.

- **Right to complain to the relevant data protection authority(ies)**
  The FDPIC may investigate cases in more detail on his own initiative or at the request of a third party (see article 29 para. 1 DPA).

- **Other key rights – please specify**
  There are no other key rights.

### 6 Registration Formalities and Prior Approval

#### 6.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?

Cross-Border Data Transfer: if personal data are transferred to a...
country that has no adequate data protection laws in force, additional safeguards are necessary. Safeguards are, for example, data transfer agreements or group-wide data protection policies (for transfers within a group of companies). The FDPIC must be informed about these safeguards prior to transborder disclosure (see article 6 para. 3 DPA and article 6 para. 1 ODPA).

Registration of Data Files with the FDPIC: federal bodies must register their data files with the FDPIC (see article 11a para. 2 DPA). Private persons must register their data files with the FDPIC only if: 1) they regularly process sensitive personal data or personality profiles; or 2) they regularly disclose personal data to third parties (see article 11a para. 3 DPA). Exceptions from the registration duty are set out in article 11a para. 5 DPA and in article 4 ODPA (for example, if the respective legal entity has appointed an internal Data Protection Officer who monitors compliance with data protection laws).

6.2 If such registration/notification is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?

The registration/notification must include both specific but also general information (for further details, see the answer to question 6.5 below).

6.3 On what basis are registrations/notifications made (e.g., per legal entity, per processing purpose, per data category, per system or database)?

See the answer to question 6.1 above. The registration of data files is made per data file.

6.4 Who must register with/notify the data protection authority (e.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation)?

Generally, the local legal entity is the Data Controller who transfers personal data pursuant to the DPA abroad (see the definition in the answer to question 2.1 above) and/or is the Controller of the Data File (see the definition in the answer to question 2.1 above). Foreign entities domiciled outside of Switzerland may be qualified as Controllers of the Data File in the sense of the DPA. However, the FDPIC is not able and does not enforce the DPA in the case of a foreign legal entity domiciled outside of Switzerland because of the principle of territoriality. In case a foreign legal entity is the Controller of the Data File with personal data of Swiss data subjects, the FDPIC may investigate whether a legal entity in Switzerland is co-controller of the respective data file. The representative or branch office of a foreign Controller of the Data File is not automatically subject to the registration obligation. The representative or branch office of a foreign entity is usually not to be qualified as Controller of the Data File, since often they do not have the power to decide on the content or purpose of a data file.

6.5 What information must be included in the registration/notification (e.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes)?

Cross-Border Transfers: no detailed information is required if the standard contractual clauses of the EU or the FDPIC are used, but the communication must include the country to which the data will be transferred and the name(s) of the data recipient(s). Otherwise, the copy of the respective contract clauses must be disclosed to the FDPIC.

Data Files: information regarding the notifying entity, contact person for information requests, categories of personal data, categories of data subjects, categories of data recipients, categories of persons having access to the data files and processing purposes must be disclosed. The FDPIC provides a template registration form on its website.

6.6 What are the sanctions for failure to register/notify where required?

Upon complaint, the respective entities or individuals may be fined if they wilfully infringed the registration obligation (see article 34 para. 2 DPA). The fine can be up to CHF 10,000.

6.7 What is the fee per registration/notification (if applicable)?

There is no fee for the registration of data files or cross-border transfer notifications.

6.8 How frequently must registrations/notifications be renewed (if applicable)?

The registration must be renewed as soon as the notified information changes. There is, however, no strict deadline and the update can be executed electronically.

6.9 Is any prior approval required from the data protection regulator?

There is no such obligation. Regarding federal and cantonal authorities, such approval obligations may arise out of specific public law.

6.10 Can the registration/notification be completed online?

Yes, the notification can be completed online, but the confirmation must be signed by an authorised representative and returned by courier to the FDPIC.

6.11 Is there a publicly available list of completed registrations/notifications?

Yes, the publicly available list can be accessed via the website of the FDPIC (https://www.edoeb.admin.ch/edoeb/en/home/data-protect ion/handel-und-wirtschaft/entreprises/anmeldung-einer-datensamm lung.html).

6.12 How long does a typical registration/notification process take?

The registration process usually takes between one and two weeks.

Cross-Border Transfers: no detailed information is required if the
7 Appointment of a Data Protection Officer

7.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.

The appointment of a Data Protection Officer is optional.

7.2 What are the sanctions for failing to appoint a Data Protection Officer where required?

There are no sanctions.

7.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect of his or her role as a Data Protection Officer?

There are no specific provisions in the DPA in this regard; thus, the general rules and principles based on the Swiss Code of Obligations will apply.

7.4 Can a business appoint a single Data Protection Officer to cover multiple entities?

Yes, a single officer may cover multiple entities.

7.5 Please describe any specific qualifications for the Data Protection Officer required by law.

Independence (performs his/her function without instructions from the Controller of the Data File); sufficient resources with respect to skills and time; sufficient personal and organisational power (as he/she must have access to all data files, data processing and information thereto) (see article 12a para. 2 and article 12b para. 2 ODPA).

7.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?

Monitoring the processing of personal data and suggesting corrective measures if data protection regulations should not be complied with, and maintaining a list of all data files (see article 12b para. 1 ODPA).

7.7 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?

Yes (see article 12a para. 1 lit. b ODPA).

7.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?

No, there is no such requirement under the DPA.

8 Appointment of Processors

8.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?

Yes, an agreement with the processor is required.

8.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?

The agreement must not necessarily be in writing, but it must ensure that the data are processed only in the manner permitted for the instructing party itself and is not prohibited by a statutory or contractual duty of confidentiality. In particular, the instructing party must ensure that the processor guarantees data security.

9 Marketing

9.1 Please describe any legislative restrictions on the sending of electronic direct marketing (e.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?).

With regard to marketing communications distributed by telephone, email or fax, article 3 lit. u of the Unfair Competition Act prohibits the sending of such communication if the recipient has declared in the official telephone registry that he/she does not wish to receive such communication.

Regarding mass emails and text messages, article 3 lit. o of the Unfair Competition Act requires that such communication is only sent with the prior consent of the recipients and with information on a simple opt-out procedure. An exception is made if the entity received the contact information in connection with the sale of products or services it has purchased before and if the customer was informed at the moment of the data collection about the simple opt-out procedure. In that case, information regarding similar products or services may be sent without prior consent.

9.2 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.).

Article 3 lit. u of the Unfair Competition Act prohibits marketing communication via telephone, email and fax if the recipient has declared in any telephone registry that he/she does not wish to receive such communication. In addition, there are several industry-related “do not contact” lists (such as codes of conduct), which many companies respect but which are not mandatory.

9.3 Do the restrictions noted above apply to marketing sent from other jurisdictions?

Yes, they also apply to marketing sent from other jurisdictions.
9.4 Is/are the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?

In Switzerland, it is the State Secretariat for Economic Affairs (“SECO”) which is the competent authority to file a claim in case of violation of the interests of many persons (article 10 para. 3 of the Unfair Competition Act). The consumers’ organisations can also file claim. In addition, the FDPIC regularly issues guidelines on data protection aspects of marketing practices. Finally, article 45a of the Swiss Telecommunication Act foresees that Providers of telecommunications services shall combat unfair mass advertising.

9.5 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?

Yes, it is lawful to purchase marketing lists from third parties. The “SDV Schweizer Dialogmarketing Verband” is the leading association regarding dialogue marketing in Switzerland. The association’s members are bound by an ethics code, which is accessible by the public (http://sdv-konsumenteninfo.ch/selbstregulierung/2012_sdv_ehrenkodex/).

9.6 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?

In case of intentional misconduct, the respective entity (respectively, the responsible person) may be sanctioned, upon request, with a prison term of up to three years or a monetary penalty of up to CHF 1,080,000 (see article 23 of the Unfair Competition Act). The effective sanctions would, of course, be much lower than the maximum penalties. There is no penalty in case of negligent misconduct.

10 Cookies

10.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).

Swiss law does not require an explicit opt-in regarding cookies. It is sufficient to inform the website users about cookies, the data processed by cookies, the purpose of processing and opt-out mechanisms (see article 45c of the Swiss Telecommunication Act).

10.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?

No, there is no distinction between different types of cookies.

10.3 To date, has/have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?

No. The FDPIC investigates new trends regarding cookies on a regular basis but has not taken any action, since cookies are not regulated in the DPA.

10.4 What are the maximum penalties for breaches of applicable cookie restrictions?

A fine not exceeding CHF 5,000 for a non-compliant cookies policy on websites of Swiss providers (see article 53 of the Telecommunication Act).

11 Restrictions on International Data Transfers

11.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.

International or cross-border disclosure means any transfer of personal data abroad, including allowing examination (e.g., of an online database), transfer or publication (see article 3 lit. f DPA). Personal data must not be disclosed abroad if the personal integrity of the persons concerned would thereby be seriously harmed (see article 6 para. 1 DPA). A serious violation of personal integrity is assumed if there is no legislation ensuring an adequate level of protection in the country where the data are disclosed.

The conditions covering disclosure of data abroad are applicable irrespective of whether the transfer takes place within the same corporate body or to another legal entity.

11.2 Please describe the mechanisms businesses typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).

The assumption that personal integrity is violated by a disclosure of personal data to a country without appropriate data protection laws can only be refuted if at least one of the minimum conditions stipulated in article 6 para. 2 lit. a to lit. g DPA is present. However, the possibility of justifying the admissibility of the international data transfer based on the general grounds for justification (according to article 13 DPA) is not available.

As a rule of thumb, all countries which have either ratified the ETS 108 agreement or are subject to the EU’s General Data Protection Regulation are considered to have an adequate level of data protection according to Swiss legislation.

In addition, the FDPIC has prepared a non-binding list of those countries whose data protection legislation should ensure appropriate protection.

However, additional precautions according to article 6 para. 2 DPA may be advisable. The transfer of data abroad within a group of companies is also permissible to countries without an adequate level of data protection if the companies concerned are subject to group-wide data protection rules which ensure appropriate protection. This regulation privileges international data transfers within a group of companies (article 6 para. 2 lit. g DPA).

Data protection rules which ensure adequate protection must at least contain the elements recommended by the FDPIC for international data transfers; namely:

- list of purposes of use split up according to categories of personal data;
11.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.

There is no general requirement to register or notify or apply for approval. The FDPIC has to be notified only in two instances:

- The FDPIC has to be informed of the fact that adequate contractual guarantees (article 6 para. 2 lit. a DPA) have been concluded or that data protection rules within the group of companies (article 6 para. 2 lit. g DPA) have been implemented. As long as the contractual guarantees are in line with the provisions in the EU standard contractual clauses, the respective data protection agreement does not have to be submitted. The group internal rules also need to be submitted to the FDPIC (article 6 para. 2 DPA). The use of the EU standard contractual clauses also facilitates the notification of the cross-border transfer to the FDPIC (see the answer to question 11.3 below).

- Most legal entities use the EU standard contractual clauses as sufficient safeguards in the sense of article 6 para 2 lit. a DPA. The use of the EU standard contractual clauses also facilitates the notification of the cross-border transfer to the FDPIC (see the answer to question 11.3 below).

12.1 What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?

There are no specific legislation or provisions under Swiss law on whistle-blowing as such. Any whistle-blower hotlines must, however, comply with the general requirements of the DPA. There are ongoing attempts to regulate whistle-blowing and to provide protection for whistle-blowers. Currently, the protection of the employee as a whistle-blower is very weak. The employee is potentially exposed to civil (e.g., termination of his/her job, potential damages) and criminal (e.g., offences due to false allegations, industrial espionage) sanctions. There are no restrictions as such to what can be reported to the whistle-blower hotline.

12.2 Is anonymous reporting prohibited, strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do businesses typically address this issue?

There are no provisions prohibiting or discouraging anonymous reporting. In practice, it is, however, often recommended not to report anonymously. The main argument in favour of non-anonymous reports is the transparency principle in article 4 para. 4 DPA (see the answer to question 4.1 above). Swiss doctrine is mainly of the opinion that companies with whistle-blower hotlines do not have to register the respective data collections, because there are usually no sensitive personal data or personality profiles of employees among such data and, even if there is such sensitive personal data, it is not processed on a regular basis.

Whistle-blowing is mainly discussed in Switzerland in connection with the loyalty and confidentiality duties of the employee, the provisions regarding justified termination, and the employer’s duty of care towards its employees. The employer must implement all necessary measures in order to ensure that the personality rights of the whistle-blower are not infringed. Accordingly, the employee must be informed transparently and comprehensively about all aspects of the whistle-blower hotline (where it is operated, who is operating it, etc.) and of the consequences his/her whistle-blowing activities may have before using the hotline.

13.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?

No, there is no general requirement to register/notify or obtain prior approval for the use of CCTV. However, if CCTV also records activities on public ground (e.g., it records activities on a private parking lot but also covers the nearby public walkway), cantonal or local data protection laws may require separate approval from the cantonal authorities.
14 Employee Monitoring

14.1 What types of employee monitoring are permitted (if any), and in what circumstances?

In accordance with the DPA and article 328b of the Swiss Code of Obligation, the employee must be previously and transparently informed about the type and method of the electronic monitoring, the scope and period of timeframe of the monitoring and its purpose.

Anonymous monitoring (including monitoring of search strings) of, e.g., employees’ use of company-provided information technology according to email and internet user guides or other policies is permissible. Pseudonymous monitoring (i.e., an abbreviation for an employee known only to a very limited group of persons) is only permissible for spot checks. No continuous monitoring is permissible in this case.

In both cases, the employees must be informed of the fact that their information technology use can/will be monitored. They may be informed via monitoring policies.

Systematic and permanent monitoring of the information technology use of specific employees is not permitted, unless: (a) the employee has consented thereto; or (b) if there is no consent, then the following requirements have to be fulfilled: (i) justified suspicion of a criminal offence; (ii) monitoring and reading of emails is necessary to confirm or dispel suspicion; (iii) conserving evidence; and (iv) there is no overriding interest of the employee. If there is an overriding interest, then the consent of the employee must be obtained. Please note that any evidence not collected in compliance with applicable law may not be admissible in court.

Accordingly, the use of so-called spyware, which clandestinely monitors the conduct of a specific employee in the workplace (e.g., computer screen movements), is not permitted and would infringe Swiss law. According to the FDPIC, this also applies to so-called content scanners (if done clandestinely). A content scanner is software that evaluates/scans sent and received emails in accordance with pre-defined keywords and reacts accordingly (cancellation or blocking of emails, etc.).

Clandestine and not pre-announced monitoring is prohibited and cannot be justified by an overriding interest of the employer. Finally, there are also specific provisions concerning the monitoring of employees in the labour laws.

14.2 Is consent or notice required? Describe how employers typically obtain consent or provide notice.

See the answer to question 14.1 above: yes, prior transparent information is required; however, consent is generally not necessary.

14.3 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?

The representatives of the employees in a company have a right to timely and comprehensive information by the company on all matters that allow employees to duly perform their tasks (article 9 of the Federal Act on Information and Participation of Employees in Companies). Since employee monitoring may have an impact on employee performance, employee representatives need to be kept up to date on this subject. However, there is no requirement to consult any entities.

15 Data Security and Data Breach

15.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?

Yes, according to article 7 para. 1 DPA, “personal data must be protected against unauthorised processing through adequate technical and organisational measures”.

Moreover, article 8 ODPA provides details on the level of security: anyone who, as a private individual, processes personal data or provides a data communication network shall ensure the confidentiality, availability and integrity of the data in order to ensure an appropriate level of data protection.

(1) In particular, he/she shall protect the systems against the following risks:

a) unauthorised or accidental destruction;

b) accidental loss;

c) technical faults;

d) forgery, theft or unlawful use; and

e) unauthorised alteration, copying, access or other unauthorised processing.

(2) The technical and organisational measures must be adequate. In particular, they must take account of the following criteria:

a) the purpose of the data processing;

b) the nature and extent of the data processing;

c) an assessment of the possible risks to the data subjects; and

d) the technological state of the art.

(3) These measures must be reviewed periodically.

Finally, article 9 ODPA states:

(1) The Controller of the Data File shall, in particular for automated processing of personal data, take the technical and organisational measures that are suitable for achieving the following goals, in particular:

a) entrance control: unauthorised persons must be denied access to facilities in which personal data are being processed;

b) personal data carrier control: unauthorised persons must be prevented from reading, copying, altering or removing data carriers;

c) transport control: on the disclosure of personal data as well as during the transport of data carriers, the unauthorised reading, copying, alteration or deletion of data must be prevented;

d) disclosure control: data recipients to whom personal data are disclosed by means of devices for data transmission must be identifiable;
e) storage control: unauthorised storage in the memory as well as the unauthorised knowledge, alteration or deletion of stored personal data must be prevented;

f) usage control: the use by unauthorised persons of automated data processing systems by means of devices for data transmission must be prevented;

g) access control: the access by authorised persons must be limited to the personal data that they require to fulfill their task; and

h) input control: in automated systems, it must be possible to carry out a retrospective examination of what personal data was entered at what time and by which person.

(2) The data files must be structured in a way that data subjects are able to assert their right of access and their right to have data corrected.

15.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

No, there is no statutory duty to do so. However, based on the general principles of the DPA, e.g., the transparency principle, it is advisable to notify the data subjects about such a breach.

15.3 Is there a legal requirement to report data breaches to affected data subjects? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

See the answer to question 15.2 above.

15.4 What are the maximum penalties for data security breaches?

There are no penalties for security breaches in the DPA. If the security breach also represents a breach of an obligation of secrecy, other legislation may be applicable and penalties may apply.

16 Enforcement and Sanctions

16.1 Describe the enforcement powers of the data protection authority(ies).

<table>
<thead>
<tr>
<th>Investigatory Power</th>
<th>Civil/Administrative Sanction</th>
<th>Criminal Sanction</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monetary penalty notices</td>
<td>This is not applicable.</td>
<td>This is not applicable.</td>
</tr>
<tr>
<td>Recommendations</td>
<td>The FDPIC can investigate cases and request the production of files, obtain information and arrange for processed data to be shown to him. If the investigation reveals that the DPA is being breached by federal bodies, the FDPIC can recommend that the federal body concerned change the method of processing or abandon the processing.</td>
<td>This is not applicable.</td>
</tr>
</tbody>
</table>

16.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?

The FDPIC can issue recommendations regarding the set-up of specific processing activities. These may include the recommendation to ban certain processing activities or to amend a processing activity. If the party concerned does not follow the issued recommendations or rejects them, the FDPIC may involve a federal court. The court’s decision will be binding for the parties, subject to appeal to the Federal Supreme Court.

16.3 Describe the data protection authority’s approach to exercising those powers, with examples of recent cases.

The FDPIC issues its recommendations on a regular basis and publishes them on his website (www.edoeb.ch).

16.4 Does the data protection authority ever exercise its powers against businesses established in other jurisdictions? If so, how is this enforced?

Yes, the FDPIC also uses its power against companies established in other jurisdictions provided that a predominant connection to Switzerland exists. Based on this principle, the FDPIC, e.g., performed an investigation and issued recommendations in the context of Google Street View against Google, Inc. (together with Google’s Swiss subsidiary) as well as in the context of Windows 10 against Microsoft Corporation (www.edoeb.ch).
17 E-discovery / Disclosure to Foreign Law Enforcement Agencies

17.1 How do businesses typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?

It depends on whether these requests are made during pending proceedings or outside of such proceedings. During pending proceedings, the companies are not permitted to (directly) respond to such requests. The foreign law enforcement agency must contact the competent Swiss authorities within the international judicial assistance (in civil or criminal matters) system. The Swiss authority then collects and transfers the respective information by way of judicial assistance to the foreign authority. The DPA is not applicable in the case of judicial assistance proceedings (see article 2 para. 2 lit. c DPA).

If a Swiss company is directly approached by a foreign law enforcement agency, the request must be qualified as outside of a pending proceeding and the DPA must be complied with. The legal person may only disclose the information and personal data to the foreign authority if the DPA is complied with, in particular with article 6 DPA regarding cross-border data transfers.

The so-called Swiss blocking statutes (e.g., articles 271 and 273 of the Swiss Criminal Code) are most relevant in this context. Due to the blocking statutes, companies within Switzerland cannot comply with foreign e-discovery requests without incurring the risk of a penal prosecution for unpermitted disclosure. It must be decided on a case-by-case basis whether such requests can be complied with or whether a specific waiver from the competent authorities must be obtained (if applicable). If a Swiss company violates the blocking statutes, its members of the board might be sanctioned with a fine or imprisonment.

17.2 What guidance has/have the data protection authority(ies) issued?

The FDPI has issued a guidance regarding this subject matter. Basically, the guidance comes to the same conclusions as set out in the answer to question 17.1 above.

18 Trends and Developments

18.1 What enforcement trends have emerged during the previous 12 months? Describe any relevant case law.

The Swiss Federal Supreme Court dealt with the implementation of video surveillance by the police (Decision 6B_181/2018 of 20 December 2018). The Swiss Federal Supreme Court ruled that such surveillance is a coercive measure that should be ordered by the prosecution with the approval of the specific court responsible for monitoring coercive measures. The employer’s agreement to monitor its employees suspected of theft does not constitute consent to the implementation of such a measure. Once the police have installed the video surveillance without respecting these legal requirements, the information collected is absolutely inoperable and must be destroyed.

The Swiss Supreme Court also ruled in a new decision (Decision 6B_91/2018 of 27 December 2018) with regard to the exchange of personal data collected during a criminal proceeding. The Swiss Federal Supreme Court confirmed the lower court’s decision, according to which, the criminal justice authority may disclose personal data from pending proceedings for use in other criminal, civil or administrative pending proceedings provided that the data may provide essential information and is not contrary to any overriding public or private interests, according to article 96 and article 101 para. 2 of the Swiss Criminal Procedure Code. In the case at hand, the Attorney General issued, during a criminal investigation, a freezing order on the sum of CHF 7,000, which the accused had won at the casino two days prior to the attachment. Since the Attorney General was aware that the accused was subject to several certificates of shortfall, it decided to inform the debt collection office of the seized assets. Upon the debt collection office’s request, the Attorney General then transferred the seized assets in order for them to be part of the attachment proceedings.

18.2 What “hot topics” are currently a focus for the data protection regulator?

The following hot topics are currently a focus:

- Swiss-US Privacy Shield.
- Revision of the DPA.
- Revision of the legal basis for the surveillance by insurers.
- Big Data, in particular for healthcare research and platforms.
- CCTV monitoring.
- Data protection and personalised healthcare.
- Data protection and drones used by individuals for private purposes.
- Dashcams (small video recorders often used in cars).
- Transmission of data to US authorities based on the US Program for Swiss banks (ongoing decisions from the Swiss Federal Supreme Court).


In September 2017, the Federal Council submitted a draft of the revised DPA to parliamentary discussions, which are currently ongoing. It is not yet clear when the revised act will come into effect. The goal of this revision is, among others, to strengthen data protection provisions to reflect evolving technological and social circumstances. In this respect, a key objective is to align Swiss data protection laws with European legislation (Regulation (EU) 2016/679 and Directive 2016/680) in order to facilitate continued transborder data flows and to comply with the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention ETS No. 108). Further, companies will be obliged to take steps to prevent potential data breaches whenever personal data are processed.
Lorenza Ferrari Hofer is head of Pestalozzi’s IP&TMT Group and co-head of the Life Sciences Group. She specialises in intellectual property, unfair competition, data law, data protection and contract law. Lorenza Ferrari Hofer has years of experience in structuring complex R&D, know-how transfer and cooperation projects, particularly in the field of life sciences. She assists technology corporations as well as research institutions in both negotiations and strategic matters, and represents them in legal proceedings in front of Swiss courts, arbitral tribunals and regulatory authorities. In addition, Lorenza Ferrari Hofer has a broad knowledge of media, advertising and entertainment matters where she regularly represents and advises companies and individuals in respect of copyright, unfair competition and privacy law issues. Lorenza regularly lectures and publishes in the fields of international licensing and technology transfer, and in several areas of unfair competition, data protection law and intellectual property law. She is consistently recommended by the leading directories of the legal profession, such as The Legal 500, Chambers & Partners, Who’s Who Legal, WIPR Leaders and IAM. Her professional languages are German, Italian, English and French.

Pestalozzi supports international and domestic clients in all aspects of Swiss law from our offices in Zurich and Geneva. The firm is known for integrity, the highest quality standards and proven effectiveness. Clients benefit from the know-how of over 120 partners, attorneys and support staff. With practice groups and expertise in all areas of business law, Pestalozzi forms customised teams to meet every challenge. Pestalozzi’s contacts include an international network of lawyers who give you access to top-quality law firms in jurisdictions worldwide. The care of clients is the focus of everything we do at Pestalozzi, supported by the diversity of our people and a dynamic company culture that ensures a creative, practical and effective response in every case. Pestalozzi’s main clients are large domestic and foreign corporations. We also assist medium-sized companies and private individuals. The broad range of sectors it serves includes financial services as well as a vast array of industries ranging from automobiles to watches.
Taiwan

Lee and Li, Attorneys At Law

1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

The main statute governing personal data protection in Taiwan is the Personal Data Protection Act (“PDPA”). The Enforcement Rules of the Personal Data Protection Act (the “Enforcement Rules”) provide further guidelines on interpretation and implementation of the PDPA. The PDPA was first introduced in Taiwan in 1996 and was significantly amended and renamed in 2010, with the amendments becoming effective in 2012. Other than the PDPA and the Enforcement Rules, the central competent authorities for quite a few industries have also stipulated the rules with regard to the relevant security matters for such industries. The framework of the PDPA is similar to that of the privacy legislation of the EU.

1.2 Is there any other general legislation that impacts data protection?

The Constitutional Court, Judicial Yuan, once issued an interpretation which confirmed that the “privacy right” is one of the basic human rights protected under our constitution. Meanwhile, the Civil Code offers general protection on the right to privacy, under which people can bring tort claims for infringement of privacy. Under the Criminal Code and the Communication Security and Surveillance Act, privacy and secrecy of communications are further protected.

1.3 Is there any sector-specific legislation that impacts data protection?

Under the PDPA, each central competent authority of a particular industry has the power to stipulate further rules concerning the “security and maintenance plan for personal information files” and the “disposal measure for personal data after a business terminates operation” for that industry. For example, the central competent authority for online retail business has stipulated such rules for this sector. Some other statutes also stipulate data-related matters, such as the Financial Holding Company Act (with regard to cross-selling activities) and the Pharmaceutical Affairs Act (concerning a drug safety surveillance and reporting system).

1.4 What authority(ies) are responsible for data protection?

The National Development Counsel (“NDC”) is the authority that is currently in charge of interpreting the PDPA. The NDC also acts as a coordinator among different government authorities with regard to the interpretation and implementation of personal data protection matters. The NDC established a Personal Data Protection Office in July 2018 in order to perform the relevant tasks. Another important mission of the Personal Data Protection Office the NDC is to obtain the “adequacy decision” from the EU authority concerning the GDPR. The negotiation commenced in spring 2018. Meanwhile, the central competent authority of each industry and the local (city and county) government authorities are granted the power to enforce certain matters stipulated under the PDPA, such as stipulating rules with regard to the “security maintenance” of personal data, carrying out audits and inspections, and imposing rectification orders and administrative penalties on the companies they are regulating.

2 Definitions

2.1 Please provide the key definitions used in the relevant legislation:

- **“Personal Data”**
  The PDPA defines “personal data” as a natural person’s name, date of birth, national ID card number, passport number, appearance, fingerprints, marital status, family background, educational background, occupation, contact information, financial status, social activities, sensitive data (defined below) and any other information that may be used to directly or indirectly identify a natural person.
- **“Processing”**
  According to the PDPA, “processing” means recording, inputting, storing, editing, correcting, duplicating, indexing, deleting, outputting, linking or internal transmission of personal data for the purpose of setting up or utilising personal information files.
- **“Controller”**
  The PDPA does not use the term “controller” in its text but it adopts similar concepts. Under the PDPA, government and non-government agencies are separately referred to when the text needs to describe the relevant “controller”. The PDPA defines a “non-government agency” broadly to include any natural person, juristic person and unincorporated association which is not a government agency.
Do the data protection laws apply to businesses established in Taiwan?

Key Principles

“Processor”

Again, the PDPA does not use the term “processor” in its text but it adopts similar concepts. Under the PDPA, when a person/entity collects, processes, and/or uses personal data under the commission or on behalf of others, such a person/entity will be regulated in a way similar to the “processor” being regulated under the GDPR, although with far fewer regulatory burdens.

“Data Subject”

A “data subject” is a natural person whose personal data is collected, processed, or used.

“Sensitive Personal Data”

Sensitive personal data include personal data with regard to medical history, medical treatments, genealogy, sex life, health-check results and criminal records.

“Data Breach”

The PDPA does not use the term “data breach” in its text. The relevant description under the PDPA is an incident under which personal data are stolen, disclosed, altered or infringed in other ways due to the violation of the PDPA.

Other key definitions – please specify (e.g., “Pseudonymous Data”, “Direct Personal Data”, “Indirect Personal Data”)

Indirectly Identifiable: The Enforcement Rules stipulate that whether an individual is “indirectly identifiable” depends on whether or not a government or non-government agency is in possession of or has access to other data, and thereby is able to identify the individual by comparing, combining, or connecting the data collected with such other data.

Lawful basis for processing

For government agencies, lawful bases for processing include: (i) processing that is provided by law; (ii) having the consent of the data subject; and (iii) processing that will not be detrimental to the rights or interests of the data subject. For non-government agencies, lawful bases for processing include: (i) processing that is provided by law; (ii) having/negotiating a contract between the non-government agency and the data subject, and appropriate security measures have been adopted therefor; (iii) processing of the data that is already in the public domain due to disclosure by the data subject or in a legitimate manner; (iv) processing that is necessary for a government agency’s performance of its statutory duties or a non-government agency’s fulfilment of legal obligations, and appropriate security measures have been or will be adopted therefor; (vi) the data is already in the public domain due to disclosure by the data subject or in a legitimate manner; (vi) processing is necessary for statistics-gathering or academic research by a government agency or academic research institution for medical, health or crime-prevention purposes, provided that any information sufficient to identify the data subject has been removed; (v) having the consent of the data subject; (vi) processing that is necessary for the furtherance of public interest; (vii) processing of the data that was collected from publicly available resources, unless the interest of the data subject takes priority over that of the collector or processor; and (viii) processing that will not be detrimental to the rights or interests of the data subject.

The PDPA does not use the term “data breach” in its text. The Enforcement Rules stipulate that whether an individual is “indirectly identifiable” depends on whether or not a government or non-government agency is in possession of or has access to other data, and thereby is able to identify the individual by comparing, combining, or connecting the data collected with such other data.

3 Territorial Scope

3.1 Do the data protection laws apply to businesses established in another jurisdiction be subject to those laws?

The PDPA does not spell out any extra-territorial effect in its text, although one of the articles does refer to the situation where a company with no presence in Taiwan may be sued in Taiwan due to a violation of the PDPA. The current position of the authority is that if the activities concerning data collection or processing are conducted in Taiwan, the PDPA will become applicable even if the business conducting such activities does not have a presence in Taiwan. It is still uncertain whether “cross-border” collection and use of personal data via the Internet would be deemed as collecting and using the personal data in Taiwan.

4 Key Principles

4.1 What are the key principles that apply to the processing of personal data?

Transparency

A controller is required to notify the data subject of the matters specified under Article 8 or 9 of the PDPA, which in general include: (i) the identity of the controller; (ii) the purposes of the collection; (iii) the type of data collected; (iv) the term, place and method of use and the persons who may use the data; (v) the data subject’s rights and the manner in which such rights may be exercised; (vi) the consequences of his or her failure to provide the required personal data; and (vii) the source from which the controller obtained the personal data (indirect collection).

Proportionality

This is basically the same as data minimisation. Moreover, the PDPA requires a controller to have in place appropriate security measures to prevent personal data from being stolen, altered, damaged, destroyed, lost or disclosed. The Enforcement Rules further provide certain technical and organisational measures that a controller may consider adopting based on the principle of proportionality, i.e., based on the quality and quantity of the personal data involved.

Retention

Neither the PDPA nor the Enforcement Rules prescribe any specific requirements regarding data retention. Nonetheless, the PDPA requires controllers to delete or stop collecting.
processing or using personal data voluntarily or upon the request of the data subject when the purpose(s) for which the personal data were collected cease(s) to exist or the retention period expires. The retention will be deemed to be necessary for the performance of a controller’s statutory duties or business operation if: (i) the retention period provided by law or contract has not expired; (ii) the deletion will be detrimental to the rights or interests of the data subject; or (iii) there is any other legal basis for the retention.

Other key principles – please specify
A controller must ensure the accuracy of personal data and correct or supplement personal data voluntarily or upon the request of the data subject. If the failure to provide accurate personal data was attributable to a controller, it shall notify the persons to whom the data were provided as soon as the controller corrects or supplements the data.

5 Individual Rights

5.1 What are the key rights that individuals have in relation to the processing of their personal data?

- Right of access to data/copies of data
A data subject has the right to access his or her personal data to check and review them and have a copy of the data.

- Right to rectification of errors
A data subject has the right to correct or supplement his or her personal data. A controller must cease the processing or use of personal data if there is any dispute over the accuracy of personal data, unless (i) the processing or use is necessary for the performance of its statutory duties or business operation, or (ii) the data subject has given written consent and the dispute has been recorded.

- Right to deletion/right to be forgotten
Whether the right to be forgotten indeed exists under the PDPA is still a subject of debate. However, Article 3 of the PDPA explicitly states that a data subject shall have the right to request a controller to delete his/her personal data.

- Right to object to processing
Under the PDPA, there is no “right to object to processing” as defined under the GDPR. However, Article 3 of the PDPA explicitly states that a data subject may request a controller to stop processing his/her personal data.

- Right to restrict processing
There is no such right in Taiwan.

- Right to data portability
There is no such right in Taiwan.

- Right to withdraw consent
It is not specified under the PDPA that a data subject may withdraw consent, but a data subject should be able to withdraw consent if it is so permitted under the Civil Code.

- Right to object to marketing
A data subject may object to marketing at any time and a business shall stop any and all marketing activities towards such a data subject at once. Meanwhile, when a business contacts a data subject for marketing purposes for the first time, the business shall provide a mechanism for the data subject to object to the marketing free of charge.

- Right to complain to the relevant data protection authority(ies)
This right is not spelled out in black and white under the PDPA but, under the Taiwan legal system, a data subject may always raise any complaint with the relevant competent authorities for any breach of the PDPA.

Other key rights – please specify
There are no other key rights in particular.

6 Registration Formalities and Prior Approval

6.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?

There is no such obligation in Taiwan.

6.2 If such registration/notification is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?

This is not applicable.

6.3 On what basis are registrations/notifications made (e.g., per legal entity, per processing purpose, per data category, per system or database)?

This is not applicable.

6.4 Who must register with/notify the data protection authority (e.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation)?

This is not applicable.

6.5 What information must be included in the registration/notification (e.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes)?

This is not applicable.

6.6 What are the sanctions for failure to register/notify where required?

This is not applicable.

6.7 What is the fee per registration/notification (if applicable)?

This is not applicable.

6.8 How frequently must registrations/notifications be renewed (if applicable)?

This is not applicable.
6.9 Is any prior approval required from the data protection regulator?

This is not applicable.

6.10 Can the registration/notification be completed online?

This is not applicable.

6.11 Is there a publicly available list of completed registrations/notifications?

This is not applicable.

6.12 How long does a typical registration/notification process take?

This is not applicable.

7 Appointment of a Data Protection Officer

7.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.

The PDPA does not require a business to appoint a Data Protection Officer. The Enforcement Rules only states that a business shall allocate “sufficient” manpower to handle personal data protection matters. Hence, it is up to a business’s discretion whether to appoint a Data Protection Officer or not.

7.2 What are the sanctions for failing to appoint a Data Protection Officer where required?

This is not applicable.

7.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect of his or her role as a Data Protection Officer?

This is not applicable.

7.4 Can a business appoint a single Data Protection Officer to cover multiple entities?

This is not applicable.

7.5 Please describe any specific qualifications for the Data Protection Officer required by law.

This is not applicable.

7.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?

This is not applicable.

7.7 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?

This is not applicable.

7.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?

This is not applicable.

8 Appointment of Processors

8.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?

No. The PDPA does not mandatorily require a business to enter into any form of agreement with its processor, while the Enforcement Rules require a controller to exercise proper supervision over the processor and suggest certain supervision measures to be taken. As a result, it is advisable for a controller to stipulate such suggested supervision measures in the commission agreement with its processor, if any.

8.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?

There is no such formality requirement. Again, it is advisable for a controller to stipulate the below matters in the commission agreement with its processor:

(i) the scope, types, specific purposes and duration of such collection, processing or use;
(ii) the security measures that the processor shall adopt pursuant to the suggested level and scope as set forth under Paragraph 2, Article 12 of the Enforcement Rules;
(iii) whether the processor is allowed to further commission a sub-processor for such processing;
(iv) the specific matters for which the processor must notify the controller, and the remedial measures that must be adopted if the processor or its employee violates the PDPA or relevant regulations;
(v) the matters which are reserved for the data controller’s instructions, if any;
(vi) the data processor must return all devices containing personal data and delete personal information files stored and kept by the processor due to the performance of such commission agreement when the commission has been terminated or rescinded; and
(vii) the controller shall have the right to periodically check that the processor carries out the above-mentioned measures.
9 Marketing

9.1 Please describe any legislative restrictions on the sending of electronic direct marketing (e.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?).

Sending marketing information by email or SMS text message to data subjects constitutes the use of their personal data. A business may use personal data by sending marketing information to a data subject only if the use is compatible with the specific purpose(s) under which the data was collected, unless the use for any new purpose is legally founded; for example, the data subject has given a separate consent for this new purpose (opt-in rules). A business must immediately cease the use of personal data for such marketing purposes if the data subject has notified the business that he or she does not wish to receive such marketing information (opt-out rules).

The restrictions are the same as those outlined in question 9.1 above.

9.2 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.).

9.3 Do the restrictions noted above apply to marketing sent from other jurisdictions?

Please see the response to question 3.1 above.

9.4 Is/are the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?

No, the authorities are not very active in this regard.

9.5 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?

No, unless the data subject has specifically consented to such marketing activities; but it is hard to believe how such consent can be legally obtained.

9.6 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?

For sending marketing information without lawful basis for collection, or if the marketing activities are not within the specific purpose under which the data were collected, a business may have an administrative fine of up to NT$500,000 imposed, and will be ordered to take corrective measures; otherwise, it may be fined consecutively until correction is made.

For failure to comply with the requirement to offer a free opt-out mechanism when a business first contacts a data subject, or with the requirement for a business to stop marketing activities when the data subject raises an objection, a business will be ordered to take corrective measures within a designated time limit, and may have an administrative fine of up to NT$200,000 imposed if it fails to make corrections.

10 Cookies

10.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).

There is no specific legislation dealing with cookies under Taiwan law. If a business is able to identify any specific individual by using cookies, the cookies will be deemed as “personal data” and the business shall use the cookies in accordance with the PDPA.

10.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?

No. The PDPA does not differentiate different types of cookies. As long as they are able to identify individuals, they will be treated as personal data and the one using the cookies shall comply with the PDPA.

10.3 To date, has/have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?

No such action has been taken to date.

10.4 What are the maximum penalties for breaches of applicable cookie restrictions?

Please see the response to question 16.1 below.

11 Restrictions on International Data Transfers

11.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.

International data transfers are allowed under the PDPA, unless the central competent authorities issue any order to prohibit or restrict the international data transfer. Under the PDPA, the central competent authorities may impose restrictions on a non-government agency’s transfer of personal data abroad if: (i) the transfer would prejudice any material national interest; (ii) it is prohibited or restricted under an international treaty or agreement; (iii) the country to which the personal data are to be transferred does not afford sound legal protection of personal data, thereby affecting the rights or interests of the data subjects; or (iv) the purpose of the transfer is to evade restrictions under the PDPA.

On 25 September 2012, the National Communications Commission (“NCC”) issued a blanket order prohibiting communications enterprises from transferring subscribers’ personal data to mainland China on the grounds that the personal data protection laws in mainland China are still inadequate.

11.2 Please describe the mechanisms businesses typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).

Businesses will check whether (i) they have fulfilled their notification
Obligations to data subjects, (ii) they have a lawful basis for the transfer (internal processing or disclosure to third parties), and (iii) the transfer is compatible with the specified purpose(s).

11.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.

No, this is not required in Taiwan.

12 Whistle-blower Hotlines

12.1 What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?

There has not been any general whistle-blowing legislation under Taiwan law, although the Agency against Corruption, within the Ministry of Justice, announced a draft Whistleblower Protection Act (the “draft WPA”) on November 23, 2018. The draft WPA governs reports regarding not only public servants’ non-compliance, but also the private sector’s whistleblowing systems. However, please note that for the private sector’s non-compliance, the draft WPA only applies to non-compliance that may lead to certain criminal/administrative liabilities. There is no clear timeline for the draft WPA to be enacted. In addition, according to the current proposal, the draft WPA would not take effect until one year after it has been enacted, if it is enacted.

12.2 Is anonymous reporting prohibited, strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do businesses typically address this issue?

The existing law does not restrict anonymous reporting. However, the draft WPA will only provide protection for the individual who discloses his/her identity when making a report. If the individual makes a report without disclosing his/her identity, he/she cannot be protected by the draft WPA and claim any rights therefrom.

13 CCTV

13.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?

No. However, it is advisable to notify the public by placing a high-visibility sign.

13.2 Are there limits on the purposes for which CCTV data may be used?

Unless the CCTV data is recorded in a public place and when the data is used, the recorder does not “tag” or “identify” any individual from the data, the person recording the CCTV data would need to have any of the lawful bases as set forth under Article 19 of the PDPA (please see the response to question 4.1 above) and shall use the CCTV data within the scope of the specific purpose under which the data were collected. Otherwise, consent from the data subject shall be required.

14 Employee Monitoring

14.1 What types of employee monitoring are permitted (if any), and in what circumstances?

Employee monitoring practices are permitted if (i) the employees no longer have a reasonable expectation of privacy, and (ii) such monitoring is not expressly prohibited by law. Employees are deemed not to have a reasonable expectation of privacy if their employer has expressly announced the monitoring policy and/or employees have consented to the monitoring. Furthermore, employees are deemed to have given an implied consent if they continue to use the equipment provided by the employer after the employer has announced the monitoring policy.

14.2 Is consent or notice required? Describe how employers typically obtain consent or provide notice.

Employers may choose to issue a notice or obtain consent. Typically, employers will expressly announce the monitoring policy by sending emails and/or a written notice to each employee and publish the monitoring policy at the workplace.

14.3 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?

Only to the extent required under any employment or collective agreement.

15 Data Security and Data Breach

15.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?

The PDPA requires a controller to have in place appropriate security measures to prevent personal data from being stolen, altered, damaged, destroyed, lost or disclosed. The Enforcement Rules further provide certain technical and organisational measures that a controller may consider adopting based on the principle of proportionality, i.e., based on the quality and quantity of the personal data involved. A controller is required to supervise the activities of its processor and shall require its processor to adopt appropriate security measures based on the above principles.

15.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

The PDPA does not require the reporting of data breaches to the relevant data protection authorities.
Again, under the PDPA, each central competent authority of a particular industry has the power to stipulate further rules concerning the “security and maintenance plan for personal information files” for that industry. For example, the central competent authority for online retail businesses stipulated rules for such businesses and required them to report to the central competent authority any incident which is material and may impact the normal operation of the business or interests of numerous data subjects. There have been quite a few other central competent authorities that have issued similar rules for the industries they regulate.

15.3 Is there a legal requirement to report data breaches to affected data subjects? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

If there is an incident under which personal data are stolen, leaked, or altered, or the data subjects’ interests may otherwise be compromised because of a controller’s failure to comply with the PDPA, the controller must notify the data subjects of the incident and the remedies that the controller has adopted as soon as the controller has carried out an investigation of the incident.

15.4 What are the maximum penalties for data security breaches?

A non-government agency will be ordered by a data protection regulatory authority to rectify the breach within a time limit prescribed by the authority. If the non-government agency fails to comply with the order within such a time limit, the non-government agency and its statutory representative may each face an administrative fine of up to NT$200,000. They may also be subject to civil and criminal liabilities as described under question 16.1 below.

16 Enforcement and Sanctions

16.1 Describe the enforcement powers of the data protection authority(ies).

<table>
<thead>
<tr>
<th>Investigatory Power</th>
<th>Civil/Administrative Sanction</th>
<th>Criminal Sanction</th>
</tr>
</thead>
<tbody>
<tr>
<td>■ Access premises to conduct on-site inspections.</td>
<td>■ Civil damages based on the amount of a data subject’s actual damages. The courts may set the amount of damages at NT$500 to NT$20,000 for each incident per person if a data subject cannot prove the amount of actual damages.</td>
<td>■ Imprisonment sentence of up to five years and/or a criminal fine of up to NT$1 million for the following: (i) illegal collection, processing or use of personal data; (ii) failure to obey a central government authority’s order imposing restrictions on cross-border transfers of personal data; or (iii) illegal alteration or deletion of personal information files or employment of any other illegal means, thereby impeding the accuracy of personal information files. Nonetheless, criminal sanctions are imposed only if the offender has the intention to make unlawful profit for himself/herself or a third party or to infringe on others’ rights/interests, and there is an actual injury or threat thereof.</td>
</tr>
<tr>
<td>■ Require explanation, cooperation, or provision of relevant supporting documents.</td>
<td>■ The competent authorities may impose an administrative fine of between NT$50,000 to NT$500,000 if a non-government agency violates the relevant data protection requirements. Nonetheless, for minor violations such as failure to comply with notification requirements, the competent authority must first designate a time limit for the non-government agency to rectify the failure. Only if the non-government agency fails to rectify the failure within the time limit will the competent authorities impose an administrative fine between NT$20,000 and NT$200,000. Please note that the administrative fine mentioned above may be imposed consecutively until the violation is rectified, and both the non-government agency and its statutory representative would have an administrative fine of the same amount imposed.</td>
<td></td>
</tr>
<tr>
<td>■ Detain or copy personal data or personal information files that can be confiscated or submitted as evidence.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

16.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?

No, it has no such power.

16.3 Describe the data protection authority’s approach to exercising those powers, with examples of recent cases.

Both the central and local government authorities have the power to carry out audits and inspections on the non-government agencies. In order to audit and inspect any non-compliance, they may: (i) access the premises of non-government agencies; (ii) require information; and (iii) detain or copy personal data or personal information files that can be confiscated or submitted as evidence. If a non-government agency is found in violation of the PDPA, the authorities may impose an administrative fine and take any of the following actions: (i) prohibit the non-government agency from collecting, processing or using the personal data; (ii) demand the deletion of the personal information files already processed; (iii) confiscate or destroy the personal data illegally collected; and (iv) publicise the violation case, the name of the non-government agency, and the name of the person in charge.

Most cases are related to financial institutions. Several financial institutions have been given administrative fines for breach of confidentiality or unauthorised disclosure of customers’ data. In one case, a bank was fined because it failed to take necessary protective measures when uploading its files to a search engine, causing its customers’ data to be accessed by the general public online. In the cases involving financial institutions, the Financial Supervisory Commission (“FSC”) imposed administrative fines or sanctions in accordance with the law governing the specific industry, such as the Banking Act or the Insurance Act.
No, there have been no such cases thus far.

The disclosure and transfer of personal data to foreign law enforcement agencies constitute the use of the personal data for a new purpose, and thus require a valid legal basis for the disclosure (e.g., a use that is specifically permitted by law or based on data subjects’ separate consent). Most companies in Taiwan will reject such disclosure unless foreign law enforcement agencies have a Taiwanese court serve the request through judicial assistance, because under those circumstances, such disclosure is permitted by law.

The Taiwan authorities have not issued any guidance in this regard.

The first class action against a business for a data breach incident was brought to court in March 2018. The Consumers’ Foundation initiated a class action against a famous travel agency company for civil compensation on behalf of consumers. Thus far, the case is still initiated a class action against a famous travel agency company for civil compensation on behalf of consumers. Thus far, the case is still being heard by the district court and no decision has been made.

According to the local news, the personal data of around 360,000 consumers of the travel agency company were compromised by an phone scammers and suffered losses for being deceived. The Consumers’ Foundation claimed that the travel agency company had not taken appropriate security measures to protect their consumers’ personal data, such as restricting the staff that were authorised to access personal information files internally. The travel agency company stated that it had taken all necessary security measures to protect its personal information files, including putting up firewalls and being certified by certification organisations, and hence, it did not deem that it would have committed negligence with regard to the data breach incident and refused to settle with the consumers.

Meanwhile, the long-drawn-out “right to be forgotten” lawsuit against Google continues. A manager of a famous professional baseball team was alleged to have been involved in certain fraud cases and scandals, but was not convicted for any crime that was alleged. He changed his name thereafter. However, as long as anyone conducts a search on his name, the relevant news reports concerning the scandals and fraud cases still come up on the screen. This person exercised his right to delete personal data under the PDPA against Google Taiwan and Google LLC. The case against Google Taiwan has been terminated for the reason that Google Taiwan was not responsible for Google’s search business in Taiwan. The case against Google LLC is still being heard by the supreme court of Taiwan and no decision has been made. Google LLC claimed that the Taiwan court has no jurisdiction over it because it is not located in Taiwan. The supreme court’s decision on this will determine whether the PDPA would in any way have any extra-territorial effect or would be applicable to cross-border data collection activities via the Internet.

With regard to the case brought by certain individuals against our health authority, objecting to our health authority’s allowing researchers to access to the data in our National Health Insurance system, such as our medical records, for academic research: previously, our supreme administrative court had opined that the use of data should be deemed legal under the PDPA and the case was dismissed. The individuals filed an application with the Constitutional Court for further interpretation and, hence, the issue has again become unsettled.

Since the GDPR became effective in May 2018, society’s awareness of personal data and privacy protection has been raised once again. The government, privacy professionals, businesses, and the general public are discussing whether the PDPA should be amended so as to be compatible with the GDPR. For example, some criticised that the PDPA does not offer data subjects sufficient rights as compared with the GDPR, such as the right to be forgotten. Meanwhile, the medical industry is requesting that the government learn from the GDPR, such as the right to be forgotten. Meanwhile, the medical industry is requesting that the government learn from the GDPR, as the GDPR provides more room and channels for the industry to use sensitive personal data, such as medical records, to develop new medical treatments.

While the NDC is working on obtaining the adequacy decision from the EU; it is also reviewing and unifying the past interpretation letters issued by the Ministry of Justice (“MOJ”), the agency previously in charge of the interpretation of the PDPA; it is hoping to clarify as many issues as possible. For example, it has been clarified that under the PDPA, we will adopt the same concept of anonymisation and pseudonymisation as given in the GDPR. Some other topics are still under debate among different stakeholders; for example, whether to adopt the same right to be forgotten as the EU has, and whether the government should release the data in our National Health Insurance system to the private sector for further development and use. It is anticipated that more guidance will evolve, and that the PDPA will eventually be amended in the coming years.
Lee and Li is a full-service law firm and the largest law firm in Taiwan. Its history can be traced back to the 1940s. Lee and Li has formed practice groups which span corporate and investment, banking and capital markets, trademarks and copyright, patents and technology, and litigation and ADR. Its services are performed by over 100 lawyers admitted in Taiwan and more than 100 technology experts, patent agents, patent attorneys, and trademark attorneys. Lee and Li was recognised as the ‘Taiwan Firm of the Year’ or the ‘National Law Firm of the Year’ by IFLR in 2001–2018. In 2019, for its professional and sophisticated legal practice in the field of mergers and acquisitions and financial and capital markets, Lee and Li is named the Most Innovative National Law Firm of the Year for Taiwan by IFLR. Lee and Li has been recognised by other international institutions as the best law firm in the region, including, Who’s Who Legal, China Law & Practice, Leaders League, Chambers & Partners, Asialaw Regional Awards, among others.
Chapter 44

Turkey

Çiğdemtekin Çakırca Arancı Law Firm

Tuna Çakırca

İpek Batum

1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

The principal data protection legislation is Personal Data Protection Law no. 6698 (“PDPL”). The secondary legislation of the PDPL consists of:

- Regulation on the Deletion, Destruction or Anonymization of Personal Data, which entered into force on 1 January 2018;
- Regulation on the Data Controllers Registry, which entered into force on 1 January 2018 (“Registry Regulation”);
- Communique on the Procedures and Principles of Application to Data Controller, published by the Personal Data Protection Authority (“Authority”), which entered into force on 10 March 2018; and
- Communique on Principles and Procedures for Fulfilment of Informing Obligation, published by the Authority, which entered into force on 10 March 2018.

Additionally, guidelines and Q&As published by the Authority and decisions of the Personal Data Protection Board (“Board”) play a significant role in the interpretation and implementation of the PDPL and secondary legislation. The Board has the authority to regulate certain aspects of the PDPL and secondary legislation and to decide on specific data breaches.

1.2 Is there any other general legislation that impacts data protection?

Article 20 of the Turkish Constitution sets out that every person has the right to request protection of his/her personal data, which she/he should be informed of, have access to and be able to request the correction and deletion of such personal data. The Constitution also envisages that personal data can only be processed with explicit consent or when regulated by law.

Turkish Criminal Code no. 5237 stipulates imprisonment of persons who unlawfully deliver data to another person, or publish or acquire the same through illegal means, and those who fail to destroy personal data despite their duty to do so, prosecution of which is initiated upon a complaint.

Pursuant to Turkish Civil Code no. 4271, it is possible to claim material and moral damages due to the violation of protection of civil rights, which includes breach of the right to privacy.

Since the PDPL was prepared in parallel to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data no. 108 and EU Directive no. 95/46/EC, such legislation is also an important guide for the purpose of the interpretation of the PDPL and the secondary legislation.

1.3 Is there any sector-specific legislation that impacts data protection?

There are several sector-specific laws and regulations that impact data protection, including:

- Law on the Regulation of Electronic Commerce no. 6563;
- Banking Law no. 5411;
- Law on Bank Cards and Credit Cards no. 5464;
- Law on Turkish Civil Aviation no. 2920;
- Law on Electronic Communications no. 5809;
- Law on Internet Broadcasting and Crimes Committed through Internet Broadcasting no. 5651;
- Electronic Signature Law no. 5070;
- Law on Postal Services no. 6475;
- Law on Payment and Security Reconciliation Systems Payment Services and Electronic Money Organisations no. 6493;
- Regulation on Distance Contracts published in the Official Gazette, dated 17 November 2014, no. 29188;
- Regulation on Patient Rights published in the Official Gazette, dated 1 August 1998, no. 23420;
- Regulation on Protection and Privacy of Personal Health Data published in the Official Gazette, dated 20 October 2016, no. 29863;
- Regulation on International Health Tourism and Health of Tourists published in the Official Gazette, dated 13 July 2017, no. 30123; and

1.4 What authority(ies) are responsible for data protection?

The Authority is primarily responsible for the regulation of data protection activities and supervision of compliance therewith. The
Regulation on the Organization of the Personal Data Protection Authority regulates the duties, power and responsibilities of the Authority.

The Board is the decision-making body of the Authority, and the duties, powers and responsibilities of the Board are regulated under the Regulation on Working Procedures and Principles of the Personal Data Protection Board.

2 Definitions

2.1 Please provide the key definitions used in the relevant legislation:

- **“Personal Data”**
  Personal data includes any and all kinds of information relating to an identified or identifiable natural person.

- **“Processing”**
  Processing includes all acts performed on the personal data, including, but not limited to, collection, recording, storage, preservation, alteration, adaptation, disclosure, transfer, retrieval, making available for collection, categorisation, blocking, whether fully or partially through automatic or non-automatic means which form part of a filing system.

- **“Controller”**
  A data controller is the natural or legal person who determines the objectives and means of processing personal data and is responsible for the establishment and the management of a data recording system. Board decision dated 13 September 2018, no. 2018/106, sets out that an unidentified person cannot be a data controller.

- **“Processor”**
  A data processor is the natural or legal person who processes the personal data with the authority granted by the data controller and in the name of the data controller.

- **“Data Subject”**
  A data subject is the natural person whose personal data are processed.

- **“Sensitive Personal Data”**
  Sensitive Personal Data, i.e. Special Category of Personal Data under the PDPL, is exhaustively listed as data relating to: race; ethnic origin; political opinions; philosophical beliefs; religion, sect or other beliefs; appearance and dress; membership of an association, foundation or trade union; health; sexual life; criminal conviction and security measures; and biometrics and genetics.

- **“Data Breach”**
  A data breach is processing of any kind of data in breach of the PDPL and secondary legislation.

Other key definitions – please specify (e.g., “Pseudonymous Data”, “Direct Personal Data”, “Indirect Personal Data”).

- **“Explicit Consent”**
  Explicit consent must be informed, related to a specific issue and based on free will.

- **“Anonymisation”**
  Anonymisation is rendering personal data anonymous so that the data does not relate to an identified or identifiable natural person even through crosschecking with other data.

- **“Data Record System”**
  Data record system is defined as any recording system through which personal data are processed subject to specific criteria.

- **“Data Controllers Registry Information System”**
  The Data Controllers Registry Information System (“VERBIS”) is the online registry kept by the Authority on which certain data controllers must register.

3 Territorial Scope

3.1 Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to those laws?

The PDPL does not restrict its applicability to persons/businesses resident in Turkey/subject to Turkish law; therefore, any natural or legal persons who process data are subject to the PDPL and its secondary legislation regardless of the law under which it is established. In addition, as per the Registry Regulation, data controllers who are not resident in Turkey are also obliged to register with VERBIS through their representatives who are resident in Turkey before starting data processing.

4 Key Principles

4.1 What are the key principles that apply to the processing of personal data?

- **Transparency**
  The data processing mechanism must be clear, accessible, understandable and concrete.

- **Lawful basis for processing**
  Data must be processed lawfully and in conformity with the rules of good faith.

- **Purpose limitation**
  Data obtained and processed must only be used for specific, explicit and legitimate purposes.

- **Data minimisation**
  Processed data must be relevant and limited to what is necessary in relation to the processing purposes.

- **Proportionality**
  Data must be processed proportionally to the processing purposes.

- **Retention**
  Data must be retained only for the period that is necessary for the processing purposes or as set out in the applicable legislation.

Other key principles – please specify

- **Accuracy and Being Up to Date**
  Processed data must be accurate, and up to date if necessary.

5 Individual Rights

5.1 What are the key rights that individuals have in relation to the processing of their personal data?

- **Right of access to data/copies of data**
  Each person has the right to learn whether his/her personal data are processed, to request information, to learn the purpose of his/her data processing and whether data are used in accordance with their purposes and to know the third
6.2 If such registration/notification is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?

The registry application must be specific and include data as explained under question 6.5.

6.3 On what basis are registrations/notifications made (e.g., per legal entity, per processing purpose, per data category, per system or database)?

Registration should be made by each data controller, i.e. a natural or legal person who processes any kind of personal data.

6.4 Who must register with/notify the data protection authority (e.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation)?

Every natural and legal person, including foreign real persons and legal entities who process personal data, are obliged to register with VERBIS. Foreign entities are obliged to register through their representatives who are resident in Turkey.

6.5 What information must be included in the registration/notification (e.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes)?

A data controller is initially obliged to appoint a contact person who is responsible for responses to the requests raised by data subjects and for communication with the Authority. Upon approval of such person by the Authority, the following information must be submitted to VERBIS:

- Processing purposes.
- Group(s) of data subjects and explanations regarding data categories of such data subjects.
- Recipients to whom the personal data may be transferred.
- Personal data envisaged to be transferred abroad.
- Measures taken to safeguard the personal data.
- Maximum period of time necessitated for the processing purposes or applicable legislation.

6.6 What are the sanctions for failure to register/notify where required?

Data controllers who fail to meet the VERBIS registration obligation shall be required to pay an administrative fine ranging from TL 20,000 to TL 1,000,000.

6.7 What is the fee per registration/notification (if applicable)?

Registration is free of charge.

Prior to processing personal data, natural or legal persons are obliged to register with VERBIS as per the Registry Regulation. The Board has the authority to set forth exemptions to such obligation. Under such authority, the Board has determined in its various decisions that notaries, lawyers, political parties, trade unions, financial consultants, and data controllers whose annual average employee number is less than 50 and annual total balance sheet is less than TL 25,000,000 are exempt from registration requirements.
6.8 How frequently must registrations/notifications be renewed (if applicable)?

Any changes in the registered information should be registered with VERBIS within seven days.

6.9 Is any prior approval required from the data protection regulator?

While data uploaded to VERBIS is not subject to approval, the contact person responsible for communication is approved by the Authority.

6.10 Can the registration/notification be completed online?

VERBIS registration process is completed online.

6.11 Is there a publicly available list of completed registrations/notifications?

Yes, there is a publicly available list of completed registrations. The publicly available information in VERBIS is categorised in the form of main headings such as the identity and address of the data controller, purpose of processing, security measures and retention periods.

6.12 How long does a typical registration/notification process take?

- Contact person registration to VERBIS can be completed within two to five days.
- The data registration process depends on the scope of personal data, but a typical data registration process can be completed within one working week.

7 Appointment of a Data Protection Officer

7.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.

Unlike the General Data Protection Regulation (EU) 2016/679 (“GDPR”), the appointment of a Data Protection Officer is not regulated in the PDPL. Therefore, appointing a Data Protection Officer is optional.

7.2 What are the sanctions for failing to appoint a Data Protection Officer where required?

This is not applicable in Turkey.

7.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect of his or her role as a Data Protection Officer?

This is not applicable in Turkey.

7.4 Can a business appoint a single Data Protection Officer to cover multiple entities?

This is not applicable in Turkey.

7.5 Please describe any specific qualifications for the Data Protection Officer required by law.

This is not applicable in Turkey.

7.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?

This is not applicable in Turkey.

7.7 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?

This is not applicable in Turkey.

7.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?

This is not applicable in Turkey.

8 Appointment of Processors

8.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?

There are no legal requirements to enter into any form of agreements with a data processor. However, such an agreement is highly recommended.

8.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?

Data controllers have a duty of care in choosing, instructing and supervising data processors. Therefore, it is recommended to enter into a written agreement with data processors and to include in such agreement provisions on the security measures to be taken, retention periods and recourse rights.

9 Marketing

9.1 Please describe any legislative restrictions on the sending of electronic direct marketing (e.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?).

Pursuant to the Law on the Regulation of Electronic Commerce no. 6563 (“LREC”), electronic marketing messages by email or SMS can be sent on condition that opt-in consent of the recipient is obtained prior to communication, which may be obtained in writing...
9.2 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.).

The LREC defines electronic marketing as all messages in electronic format and lists marketing by telephone, call centres, facsimile, automatic dialling equipment and smart voice recorder systems in a non-exhaustive manner. Therefore, the restrictions explained above will also apply to the marketing messages via these means.

On the other hand, marketing via physical means such as sending post does not fall under the LREC and is subject to general rules of the PDPL.

9.3 Do the restrictions noted above apply to marketing sent from other jurisdictions?

The service provider, i.e. the sender of the electronic marketing message, is defined in the LREC as natural or legal persons engaging in electronic commercial activities regardless of whether they are subject to foreign law or Turkish law. Therefore, the restrictions explained above should be applied to electronic marketing messages sent from other jurisdictions as well.

9.4 Is/are the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?

In its decision no. 2018/119, dated 16 October 2018, the Board announced that data controllers, or data processors on behalf of data controllers, must cease electronic marketing communication if opt-in consent of the recipient is not obtained. The Board also repeated the duty of the data controller to take all necessary technical and organisational measures in order to prevent unlawful access to personal data and security thereof. In the event of non-compliance with these obligations, an administrative fine shall be imposed pursuant to Article 20 of the PDPL and that a criminal complaint shall be made against the data controller pursuant to the Turkish Criminal Code.

9.5 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?

While there are no specific restrictions in relation to the purchase of marketing lists from third parties, transfers of personal data through the purchase of marketing lists is subject to the PDPL and the explicit consent of the data subject should be obtained for the transfer. In case the personal data is transferred abroad, the foreign country to which personal data will be transferred must also have an adequate level of protection. The transfer of personal data abroad is explained in detail under section 11.

9.6 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?

As per the LREC, businesses may be exposed to administrative fines ranging between TL 1,550 and TL 31,051 (for 2019) in case of breach of the restrictions explained above. In case the marketing communications are sent to multiple recipients at once, the fines may be implemented by increasing the amount up to 10 times. Additionally, if applicable to the specific case, sanctions under the PDPL may also apply.

10 Cookies

10.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).

There are no specific legislative restrictions on the use of cookies; therefore, it is at the discretion of the data controller to publish a cookie policy. However, in case the data collected via cookies or similar technologies relate to an identifiable person, then the general principles of the PDPL shall apply. Also, EU Directive 2002/58/EC, which sheds light as to how the Authority may interpret the legal status of cookies or similar technologies, requires users’ informed consent before storing cookies on a user’s device and/or tracking them. In light of the above, it is advised for data controllers to publish cookie policies on their websites.

10.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?

No, there is no distinction made between different types of cookies.

10.3 To date, has/have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?

No, there has been no enforcement action in relation to cookies to date.

10.4 What are the maximum penalties for breaches of applicable cookie restrictions?

There is no maximum penalty for breaches of applicable cookie restrictions.

11 Restrictions on International Data Transfers

11.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.

Under the PDPL, personal data may only be transferred abroad with explicit consent of the data subject. The exception to such rule is that the foreign country to which personal data will be transferred shall have an adequate level of protection, and if an adequate level of protection is not available in such country, data controllers in Turkey and abroad may only transfer
data abroad with permission of the Board and a commitment provided to the Board undertaking security of the personal data. Pursuant to the PDPL, countries with an adequate level of protection are yet to be announced by the Board.

11.2 Please describe the mechanisms businesses typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).

Data controllers mostly prefer obtaining explicit consent from data subjects and entering into data protection agreements with data processors setting out undertakings relating to protection of personal data, retention periods and audit rights, in certain cases. Additionally, data processors choose to obtain assurances from data controllers that explicit consent from the data subject has been obtained and that there are recourse rights available relating thereto.

11.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.

For the purpose of the permission to be obtained from the Board as explained under question 11.1, the Board has published two forms of letters of undertaking: (i) to be executed when data is transferred from one data controller to another; and (ii) to be executed when data is transferred from a data controller to a data processor, each to be signed by both the transferor and transferee.

12 Whistle-blower Hotlines

12.1 What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?

Pursuant to the guidelines issued by the Authority, businesses should define each employee’s role in compliance with data protection legislation and train their employees regarding different aspects of the same. Therefore, while there are no regulations on corporate whistle-blower hotlines, businesses may establish whistle-blowing mechanisms. Additionally, public companies are obliged to establish committees for risk detection and internal audit, and detection of incompetence with data protection legislation is advised to be included within the scope of such committees’ duties.

12.2 Is anonymous reporting prohibited, strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do businesses typically address this issue?

Anonymous reporting is not prohibited or discouraged in the PDPL.

13 CCTV

13.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?

There are no specific regulations on the usage of CCTV from a data protection perspective; therefore, the general principles of the PDPL shall apply to CCTV. The PDPL does not require the explicit consent of the data subject if (i) other laws explicitly permit data processing, (ii) processing is necessary in order to protect the life or physical integrity of the data subject or another person where the data subject is physically or legally incapable of giving consent, (iii) execution or performance of an agreement between the data controller and data subject requires data processing, (iv) processing is required for the data controller to comply with its legal obligations, (v) the data subject already made such data available to the public, (vi) processing is necessary for the institution, usage, or protection of a right, and (vii) processing is required for protecting legitimate interests of the data controller as long as such processing does not breach the fundamental rights and freedoms of the data subject. In the absence of these circumstances, the data controller must obtain the explicit consent of the data subject. Where one or more of such circumstances exist, the data controller is under the obligation to inform the data subject of the identity of the data controller, processed data, the purpose of processing, transferees, means of collection of data, and which of the circumstances listed above exists.

In light of the above, data controllers may use CCTV for the purpose of protecting their legitimate interests, such as the security of certain areas. In order to fulfil their obligation to inform, data controllers which use CCTV are advised to place visible signs displaying the information stated above.

13.2 Are there limits on the purposes for which CCTV data may be used?

In addition to the consent/obligation to inform the obligation above, CCTV can only be used in case such usage is proportionate, limited to processing purposes and minimised for its present purpose, among other general principles.

14 Employee Monitoring

14.1 What types of employee monitoring are permitted (if any), and in what circumstances?

Employers collect their employees’ personal data for several reasons, such as regulatory reasons, security reasons and performance review. General rules of data protection shall be applicable to employee monitoring; i.e. explicit consent of the employee is required in the absence of the circumstances listed under question 13.1. It must be noted that all processing must comply with the general principles, such as proportionality, limitation to purpose, minimisation and protection of legitimate interests of the data controller. If data processing is not compliant with these principles, the explicit consent provided by the employee will not be valid.
E-mail monitoring is an example of a permitted extent of employee monitoring. According to the general principles of the PDPL and a ruling of the Turkish Constitutional Court, which was issued prior to promulgation of the PDPL, employers can monitor corporate e-mail accounts with the condition that they inform the employees; however, monitoring of private e-mail accounts of employees is unlikely to be justified as being in the employer’s legitimate interests.

14.2 Is consent or notice required? Describe how employers typically obtain consent or provide notice.

While employers must obtain explicit consent from employees in the absence of the circumstances stipulated under question 13.1, notice to employees as to how their personal data is processed is sufficient in case such circumstances exist.

For the purpose of the above, employers include data protection clauses in their employment agreements, whereby employees provide their explicit consent. Relating to the personal data which is processed on the basis of the circumstances stated under question 13.1, employers perform their obligation to inform through notices provided to and acknowledged by employees either electronically or manually. Employers also choose to place visible notifications in relation to any CCTV.

14.3 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?

There is no specific legislation regulating this area.

15 Data Security and Data Breach

15.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?

Yes, the PDPL states that it is the data controllers’ obligation to prevent unlawful processing of personal data and to prevent unlawful access to personal data by taking all necessary technical and organisational measures to provide an appropriate level of security. In January 2018, the Authority issued a guideline describing such technical and organisational measures, including, but not limited to, preparation of data inventory, conducting internal audits, training, registration to VERBIS, preparation of an authorisation matrix, conducting penetration tests, managing system access, retaining access logs, setting up firewalls and providing physical security of media on which data is stored.

15.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

Yes; in case of a data breach, the data controller is under the obligation to notify the data subject and the Authority of such situation as soon as possible. In Board resolution no. 2019/10, dated 24 January 2019, it is stated that “as soon as possible” should be interpreted as 72 hours and if the data controller fails to meet such period, an explanation relating to the delay must be provided to the Board. The data controller must use the Personal Data Notification Form published by the Authority for the purpose of such notification. The Board may also choose to declare such situation on its website.

15.3 Is there a legal requirement to report data breaches to affected data subjects? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

Yes; please refer to question 15.2 above. Additionally, the notification should be made to the data subject’s contact address. If providing notice to the data subject is not possible, the data controller may choose another form of notice such as publication on its official website.

15.4 What are the maximum penalties for data security breaches?

In case of failure to take necessary security measures and notify the Authority of the breach, the Board may impose an administrative fine ranging from TL 15,000 to TL 1,000,000 on the data controller.

16 Enforcement and Sanctions

16.1 Describe the enforcement powers of the data protection authority(ies).

<table>
<thead>
<tr>
<th>Investigatory Power</th>
<th>Civil/Administrative Sanction</th>
<th>Criminal Sanction</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Authority</td>
<td>Breach of obligation to inform – administrative fine ranging from TL 5,000 to TL 100,000.</td>
<td>N/A</td>
</tr>
<tr>
<td>The Authority</td>
<td>Breach of data security obligations – administrative fine ranging from TL 15,000 to TL 1,000,000.</td>
<td>N/A</td>
</tr>
<tr>
<td>The Authority</td>
<td>Failure to register with VERBIS and maintaining up-to-date registered data – administrative fine ranging from TL 20,000 to TL 1,000,000.</td>
<td>N/A</td>
</tr>
<tr>
<td>The Authority</td>
<td>Breach of the Board’s resolutions – administrative fine of TL 25,000 to TL 1,000,000.</td>
<td>N/A</td>
</tr>
<tr>
<td>Criminal Courts</td>
<td>Unlawful recording of personal data.</td>
<td>1 to 3 years of imprisonment</td>
</tr>
<tr>
<td>Criminal Courts</td>
<td>Unlawful transfer, transmission and collection of personal data.</td>
<td>2 to 4 years of imprisonment</td>
</tr>
<tr>
<td>Criminal Courts</td>
<td>Failure to destroy personal data.</td>
<td>1 to 2 years of imprisonment</td>
</tr>
</tbody>
</table>

16.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?

As per the PDPL, the Board has the duty and authority to render decisions on duties, authorities and obligations of data controllers. Therefore, the Board may issue a ban on a particular processing activity; however, decisions of the Board are administrative actions, cancellation of which can be claimed before administrative courts.
Additionally, circumstances which fall under criminal courts’ jurisdiction cannot be decided upon by the Board.

16.3 Describe the data protection authority’s approach to exercising those powers, with examples of recent cases.

Based on recent decisions in 2018 and 2019, the Authority exercises its powers upon data subject’s complaints rather than *ex officio* investigations, and the majority of decisions are related to imposing administrative fines due to unlawful transfers of personal data to third parties.

16.4 Does the data protection authority ever exercise its powers against businesses established in other jurisdictions? If so, how is this enforced?

There have been no publicly announced cases where the Authority imposed administrative fines on foreign persons; however, in its resolution no. 2019/10, the Board stated that in case of a data breach in another jurisdiction which has effects in Turkey, a foreign data controller is also under the notification obligations as mentioned under question 15.2.

17 E-discovery / Disclosure to Foreign Law Enforcement Agencies

17.1 How do businesses typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?

For foreign e-discovery requests or requests for disclosure from foreign law enforcement agencies, businesses should respond in accordance with the mutual judicial assistance treaties.

17.2 What guidance has/have the data protection authority(ies) issued?

The Authority has not yet issued any guidance on e-discovery.

18 Trends and Developments

18.1 What enforcement trends have emerged during the previous 12 months? Describe any relevant case law.

Data controllers are obliged to notify the data subjects and the Authority in case of a data breach and the Board may declare such situation on its website. The first of these data breach disclosures was published by the Authority on 4 May 2018. In this first example of the Board’s data breach announcement, a data breach occurred in a company that provides transportation services. As stated in this resolution, 103,337 customers and 900 drivers resident in Turkey have been affected by this data breach. To date, the Board has published 22 data breach disclosures, and this number is increasing after Board resolution no. 2019/10, which explains in detail the data breach disclosure procedure together with the time limitations for data breach disclosures.

18.2 What “hot topics” are currently a focus for the data protection regulator?

The Authority and data protection foundations frequently hold summits and symposiums on data protection matters. The “hot topics” discussed in such summits and symposiums are VERBIS, GDPR’s effect on innovation, data privacy aspects of artificial intelligence, big data, and blockchain.

Acknowledgment

The authors would like to thank Köksal Kaplan for his assistance in preparing this chapter. Köksal is an associate at Çiğdemtekin Çakırca Arancı Law Firm, specialising in corporate law.
Tel: +90 212 227 00 61 / Email: kkaplan@cdcalaw.com
Tuna Çakırca is a leading IT, M&A/corporate and capital markets lawyer. Her M&A experience includes representation of both sell- and buy-side clients in a wide range of sectors. She has also represented underwriters, issuers and/or selling shareholders, most recently for electricity and telecommunications companies. Additionally, Ms. Çakırca has extensive experience in representing foreign and local companies in connection with their corporate, commercial, regulatory, employment and real estate matters. She continues to assist many multinational companies in their day-to-day businesses in such areas. Prior to joining CCA, Ms. Çakırca was a senior associate at Chadbourne & Parke and prior to that she was an associate at Kinstellar and at White and Case. Tuna has been recognised as a key figure in the IT sector in Turkey and as one of the leading corporate and M&A lawyers in Turkey.

İpek Batum specialises in corporate and commercial transactions, particularly in the areas of corporate law, IT law, data protection, mergers and acquisitions as well as dispute resolution. She assists local and foreign clients both on a daily and transactional basis.
United Kingdom

White & Case LLP

1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

Since 25 May 2018, the principal data protection legislation in the EU has been Regulation (EU) 2016/679 (the “General Data Protection Regulation” or “GDPR”). The GDPR repealed Directive 95/46/EC (the “Data Protection Directive”) and has led to increased (though not total) harmonisation of data protection law across the EU Member States. Some provisions in the GDPR can be adapted in EU Member States’ national laws. Therefore, the UK Government passed the UK Data Protection Act 2018 (the “DPA 2018”), which covers those areas of the GDPR which EU Member States can add to or vary or that do not fall within EU law. The DPA 2018 came into force on 25 May 2018.

The GDPR applies in the UK until it leaves the EU, which is expected on 29 March 2019 (“Brexit”) unless an extension is agreed. The UK Government has incorporated the GDPR into the UK’s domestic law under clause 3 of the European Union (Withdrawal) Act 2018, which incorporates EU law into domestic law. Therefore, after Brexit, data protection law within the UK will remain aligned with the GDPR.

1.2 Is there any other general legislation that impacts data protection?

The Privacy and Electronic Communications (EC Directive) Regulations 2003 (as amended by the Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011) (the “PECR”) implement the requirements of Directive 2002/58/EC (as amended by Directive 2009/136/EC) (the “ePrivacy Directive”), which provides a specific set of privacy rules to harmonise the processing of personal data by the telecoms sector. In January 2017, the European Commission published a proposal for an ePrivacy regulation (the “ePrivacy Regulation”) that would harmonise the applicable rules across the EU. In September 2018, the Council of the European Union published proposed revisions to the draft. The ePrivacy Regulation is still a draft at this stage and it is unclear when it will be finalised.

1.3 Is there any sector-specific legislation that impacts data protection?

No, there is no sector-specific legislation that impacts data protection.

1.4 What authority(ies) are responsible for data protection?

The Information Commissioner’s Office (the “ICO”) is responsible for overseeing and enforcing the GDPR and the PECR. It is an independent body, which is sponsored by the Department for Digital, Culture, Media and Sport and reports directly to Parliament. In July 2016, Elizabeth Denham was appointed Information Commissioner.

2 Definitions

2.1 Please provide the key definitions used in the relevant legislation:

- “Personal Data” means any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

- “Processing” means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

- “Controller” means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

- “Processor” means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

- “Data Subject” means an individual who is the subject of the relevant personal data.

- “Sensitive Personal Data” are personal data, revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, data concerning health or sex life and sexual orientation, genetic data or biometric data.

- “Data Breach” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.
3 Territorial Scope

3.1 Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to those laws?

The GDPR applies to businesses that are established in any EU Member State, and that process personal data (either as a controller or processor, and regardless of whether or not the processing takes place in the EU) in the context of that establishment.

A business that is not established in any Member State, but is subject to the laws of a Member State by virtue of public international law, is also subject to the GDPR.

The GDPR applies to businesses outside the EU if they (either as controller or processor) process the personal data of EU residents in relation to: (i) the offering of goods or services (whether or not in return for payment) to EU residents; or (ii) the monitoring of the behaviour of EU residents (to the extent that such behaviour takes place in the EU).

Further, the GDPR applies to businesses established outside the EU if they monitor the behaviour of EU residents (to the extent such behaviour takes place in the EU).

4 Key Principles

4.1 What are the key principles that apply to the processing of personal data?

- **Transparency**
  Personal data must be processed lawfully, fairly and in a transparent manner. Controllers must provide certain minimum information to data subjects regarding the collection and further processing of their personal data. Such information must be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

- **Lawful basis for processing**
  Processing of personal data is lawful only if, and to the extent that, it is permitted under EU data protection law. The GDPR provides an exhaustive list of legal bases on which personal data may be processed, of which the following are the most relevant for businesses: (i) prior, freely given, specific, informed and unambiguous consent of the data subject; (ii) contractual necessity (i.e., the processing is necessary for the performance of a contract to which the data subject is a party, or for the purposes of pre-contractual measures taken at the data subject’s request); (iii) compliance with legal obligations (i.e., the controller has a legal obligation, under the laws of the EU or an EU Member State, to perform the relevant processing); or (iv) legitimate interests (i.e., the processing is necessary for the purposes of legitimate interests pursued by the controller, except where the controller’s interests are overridden by the interests, fundamental rights or freedoms of the affected data subjects).

  Please note that businesses require stronger grounds to process sensitive personal data. The processing of sensitive personal data is only permitted under certain conditions, of which the most relevant for businesses are: (i) explicit consent of the affected data subject; (ii) the processing is necessary in the context of employment law; or (iii) the processing is necessary for the establishment, exercise or defence of legal claims.

- **Purpose limitation**
  Personal data may only be collected for specified, explicit and legitimate purposes and must not be further processed in a manner that is incompatible with those purposes. If a controller wishes to use the relevant personal data in a manner that is incompatible with the purposes for which they were initially collected, it must: (i) inform the data subject of such new processing; and (ii) be able to rely on a lawful basis as set out above.

- **Data minimisation**
  Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which those data are processed. A business should only process the personal data that it actually needs to process in order to achieve its processing purposes.

- **Accuracy**
  Personal data must be accurate and, where necessary, kept up to date. A business must take every reasonable step to ensure that personal data that are inaccurate are either erased or rectified without delay.

- **Retention**
  Personal data must be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

- **Data security**
  Personal data must be processed in a manner that ensures appropriate security of those data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

- **Accountability**
  The controller is responsible for, and must be able to demonstrate, compliance with the data protection principles set out above.

5 Individual Rights

5.1 What are the key rights that individuals have in relation to the processing of their personal data?

- **Right of access to data/copies of data**
  A data subject has the right to obtain from a controller the following information in respect of the data subject’s personal data: (i) confirmation of whether, and where, the controller is processing the data subject’s personal data; (ii) information about the purposes of the processing; (iii) information about the categories of data being processed; (iv) information about the categories of recipients with whom the data may be shared; (v) information about the period for which the data will be stored (or the criteria used to determine that period); (vi) information about the existence of the rights to erasure, to rectification, to restriction of processing and to object to processing; (vii) information about the existence of the right to complain to the relevant data protection authority; (viii) where the data were not collected from the data subject, information as to the source of the data; and (ix) information about the existence of, and an explanation of the logic involved in, any automated processing that has a significant effect on the data subject.

  Additionally, the data subject may request a copy of the personal data being processed.
<table>
<thead>
<tr>
<th>Right to rectification of errors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Controllers must ensure that inaccurate or incomplete data are erased or rectified. Data subjects have the right to rectification of inaccurate personal data.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Right to deletion/right to be forgotten</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data subjects have the right to erasure of their personal data (the “right to be forgotten”) if: (i) the data are no longer needed for their original purpose (and no new lawful purpose exists); (ii) the lawful basis for the processing is the data subject’s consent, the data subject withdraws that consent, and no other lawful ground exists; (iii) the data subject exercises the right to object, and the controller has no overriding grounds for continuing the processing; (iv) the data have been processed unlawfully; or (v) erasure is necessary for compliance with EU law or national data protection law.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Right to object to processing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data subjects have the right to object, on grounds relating to their particular situation, to the processing of personal data where the basis for that processing is either public interest or legitimate interest of the controller. The controller must cease such processing unless it demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the relevant data subject or requires the data in order to establish, exercise or defend legal rights.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Right to restrict processing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data subjects have the right to restrict the processing of personal data, which means that the data may only be held by the controller, and may only be used for limited purposes if: (i) the accuracy of the data is contested (and only for as long as it takes to verify that accuracy); (ii) the processing is unlawful and the data subject requests restriction (as opposed to exercising the right to erasure); (iii) the controller no longer needs the data for their original purpose, but the data are still required by the controller to establish, exercise or defend legal rights; or (iv) verification of overriding grounds is pending, in the context of an erasure request.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Right to data portability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data subjects have a right to receive a copy of their personal data in a commonly used machine-readable format, and transfer their personal data from one controller to another or have the data transmitted directly between controllers.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Right to withdraw consent</th>
</tr>
</thead>
<tbody>
<tr>
<td>A data subject has the right to withdraw their consent at any time. The withdrawal of consent does not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject must be informed of the right to withdraw consent. It must be as easy to withdraw consent as to give it.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Right to object to marketing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data subjects have the right to object to the processing of personal data for the purpose of direct marketing, including profiling.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Right to complain to the relevant data protection authority(ies)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data subjects have the right to lodge complaints concerning the processing of their personal data with the ICO, if the data subject lives in the UK or the alleged infringement occurred in the UK.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Right to basic information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data subjects have the right to be provided with information on the identity of the controller, the reasons for processing their personal data and other relevant information necessary to ensure the fair and transparent processing of personal data.</td>
</tr>
</tbody>
</table>

### Registration Formalities and Prior Approval

#### 6.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?

No, there is no longer a legal obligation on businesses to register with or notify the ICO as there was under the Data Protection Act 1998 (the “DPA 1998”). This requirement has been replaced by a legal obligation on controllers (not processors) to pay a data protection fee under the Data Protection (Charges and Information) Regulations 2018 (the “2018 Regulations”) which came into force on 25 May 2018. As such, the following questions in this section will relate to the fee requirement instead of the registration requirement. It should be noted that certain businesses are exempt such as public authorities, charities and small occupational pension schemes.

In addition to the above, a controller must also keep records of its processing activities which, upon request, must be disclosed to the ICO. Furthermore, a processor must keep records of its processing activities performed on behalf of a controller.

#### 6.2 If such registration/notice is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?

The information provided to the ICO need not be too detailed. Only the information listed in question 6.5 must be provided.

#### 6.3 On what basis are registrations/notifications made (e.g., per legal entity, per processing purpose, per data category, per system or database)?

A separate fee is payable by every UK entity that acts as a controller.

#### 6.4 Who must register with/notify the data protection authority (e.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation)?

Any controller that is subject to the DPA 2018 must pay the fee to the Information Commissioner unless it is exempt.

#### 6.5 What information must be included in the registration/notice (e.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes)?

A controller must provide the ICO with the following information: contact details; number of staff; turnover for its financial year; type of organisation; and details of the data protection officer (if applicable).

#### 6.6 What are the sanctions for failure to register/notify where required?

The penalty for failing to pay the fee or paying the incorrect fee can be a maximum of 150% of the top-tier fee (see question 6.7 below).
6.7 What is the fee per registration/notification (if applicable)?

There are three tiers of fees ranging from £40 to £2,900 and the fee payable depends on the size of the business, its turnover and the type of business.

6.8 How frequently must registrations/notifications be renewed (if applicable)?

The fee is payable annually.

6.9 Is any prior approval required from the data protection regulator?

No, prior approval is not required.

6.10 Can the registration/notification be completed online?

Payment of the fee can be completed online through the ICO’s website.

6.11 Is there a publicly available list of completed registrations/notifications?

Yes, there is a public register of controllers who pay the data protection fee.

6.12 How long does a typical registration/notification process take?

As payment can be completed online through the ICO website, this process can be immediate. Other payment methods (e.g., cheques) may be slower.

7 Appointment of a Data Protection Officer

7.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.

The appointment of a Data Protection Officer for controllers or processors is only mandatory in some circumstances, including where there is: (i) large-scale regular and systematic monitoring of individuals; or (ii) large-scale processing of sensitive personal data. Where a business designates a Data Protection Officer voluntarily, the requirements of the GDPR apply as though the appointment were mandatory.

7.2 What are the sanctions for failing to appoint a Data Protection Officer where required?

In the circumstances where appointment of a Data Protection Officer is mandatory, failure to comply may result in the wide range of penalties available under the GDPR.

7.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect of his or her role as a Data Protection Officer?

The appointed Data Protection Officer should not be dismissed or penalised for performing their tasks and should report directly to the highest management level of the controller or processor.

7.4 Can a business appoint a single Data Protection Officer to cover multiple entities?

A single Data Protection Officer is permitted by a group of undertakings provided that the Data Protection Officer is easily accessible from each establishment.

7.5 Please describe any specific qualifications for the Data Protection Officer required by law.

The Data Protection Officer should be appointed on the basis of professional qualities and should have an expert knowledge of data protection law and practices. While this is not strictly defined, it is clear that the level of expertise required will depend on the circumstances. For example, the involvement of large volumes of sensitive personal data will require a higher level of knowledge.

7.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?

A Data Protection Officer should be involved in all issues which relate to the protection of personal data. The GDPR outlines the minimum tasks required by the Data Protection Officer which include: (i) informing the controller, processor and their relevant employees who process data of their obligations under the GDPR; (ii) monitoring compliance with the GDPR, national data protection legislation and internal policies in relation to the processing of personal data including internal audits; (iii) advising on data protection impact assessments and the training of staff; and (iv) co-operating with the data protection authority and acting as the authority’s primary contact point for issues related to data processing.

7.7 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?

Yes, the controller or processor must notify the data protection authority of the contact details of the designated Data Protection Officer.

7.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?

The Data Protection Officer does not necessarily need to be named in the public-facing privacy notice. However, the contact details of the Data Protection Officer must be notified to the data subject when personal data relating to that data subject are collected. As a matter of good practice, the Article 29 Working Party (the “WP29”) (now the European Data Protection Board (the “EDPB”)) recommended in its 2017 guidance on Data Protection Officers that both the data protection authority and employees should be notified of the name and contact details of the Data Protection Officer.
8 Appointment of Processors

8.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?

Yes. The business that appoints a processor to process personal data on its behalf, is required to enter into an agreement with the processor which sets out the subject matter for processing, the duration of processing, the nature and purpose of processing, the types of personal data and categories of data subjects and the obligations and rights of the controller (i.e., the business).

It is essential that the processor appointed by the business complies with the GDPR.

8.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?

The processor must be appointed under a binding agreement in writing. The contractual terms must stipulate that the processor: (i) only acts on the documented instructions of the controller; (ii) imposes confidentiality obligations on all employees; (iii) ensures the security of personal data that it processes; (iv) abides by the rules of regarding the appointment of sub-processors; (v) implements measures to assist the controller with guaranteeing the rights of data subjects; (vi) assists the controller in obtaining approval from the relevant data protection authority; (vii) either returns or destroys the personal data at the end of the relationship (except as required by EU or Member State law); and (viii) provides the controller with all information necessary to demonstrate compliance with the GDPR.

9 Marketing

9.1 Please describe any legislative restrictions on the sending of electronic direct marketing (e.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?).

The PECR requires businesses to obtain consent before sending electronic communications to individuals for the purpose of direct marketing. There are exemptions to this; however, they are very narrow. In 2017, the European Commission published a draft of the ePrivacy Regulation which, together with the GDPR, is likely to make it harder to engage in certain types of electronic direct marketing.

9.2 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.).

The PECR does not prohibit all unsolicited marketing calls. However, the UK offers an opt-out register (the Telephone Preference Service (the “TPS”). It is a legal requirement to not make unsolicited marketing calls to numbers registered in the TPS, without the consent of the relevant individual subscriber.

9.3 Do the restrictions noted above apply to marketing sent from other jurisdictions?

The PECR does not have formal extraterritoriality provisions and therefore cannot be applied where there is no nexus with the UK.

9.4 Is/are the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?

Yes. The ICO has issued a number of fines to companies that breached direct marketing laws. There has been significant focus over the 2016–2018 period on “nuisance calls”. In January 2018, the fines for contacting individuals without their consent ranged from £40,000 to £350,000.

9.5 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?

For a lawful purchase of a marketing list, the relevant individuals must have been originally informed by the seller that their data could be passed on to other businesses for marketing purposes and the individuals must have consented to that. The ICO recommends due diligence of any lists prior to purchase and, in practice, it is recommended that warranties are employed to ensure that the marketing list does not contravene these requirements.

9.6 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?

The maximum fine is £500,000, although typical fines are generally well below this level.

10 Cookies

10.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).

The PECR implements Article 5 of the ePrivacy Directive. Pursuant to Article 5 of the EU ePrivacy Directive, the storage of cookies (or other data) on an end user’s device requires prior consent (the applicable standard of consent is derived from the GDPR). For consent to be valid, it must be informed, specific, freely given and must constitute a real and unambiguous indication of the individual’s wishes. This does not apply if: (i) the cookie is for the sole purpose of carrying out the transmission of a communication over an electronic communications network; or (ii) the cookie is strictly necessary to provide an “information society service” (e.g., a service over the internet) requested by the subscriber or user, which means that it must be essential to fulfil their request.

The EU Commission intends to pass a new ePrivacy Regulation that will replace the respective national legislation in the EU Member States. The ePrivacy Regulation is planned to come into force in 2019.

10.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?

The draft ePrivacy Regulation envisages stricter consent requirements
for the use of cookies. It would prevent businesses from accessing users’ devices and collecting information unless they have either the consent of the user prior to commencing tracking, or if the information obtained by the tracking is necessary for the delivery of the service. Cookies which do not invade privacy (e.g., those which count the number of visitors to websites) would not require consent. Furthermore, under the PECR, no consent is required if the sole purpose of the cookie is carrying out the transmission of a communication or if it is strictly necessary to provide an information society service requested by the user.

10.3 To date, has/have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?

Between April 2018 and December 2018, the ICO received limited complaints about cookies, and therefore regards cookies as an area of comparatively lower concern.

10.4 What are the maximum penalties for breaches of applicable cookie restrictions?

The maximum penalty is currently £500,000. The ICO has indicated that it will largely continue to follow its established procedure of information and enforcement notices, with fines issued only in the most serious cases.

11 Restrictions on International Data Transfers

11.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.

Data transfers to other jurisdictions that are not within the European Economic Area (the “EEA”) can only take place if the transfer is to an “Adequate Jurisdiction” (as specified by the EU Commission), the business has implemented one of the required safeguards as specified by the GDPR, or one of the derogations specified in the GDPR applies to the relevant transfer. The EDPB Guidelines (2/2018) set out that a “layered approach” should be taken with respect to these transfer mechanisms. If the transfer is not to an Adequate Jurisdiction, the data exporter should first explore the possibility of implementing one of the safeguards provided for in the GDPR before relying on a derogation.

In the event of a no-deal Brexit, the UK will become a third country for the purposes of EU law. While the UK government has indicated that personal data will be able to flow from the UK to the EU as it did prior to Brexit, data may only be lawfully transferred from the EU to the UK if an adequate decision is reached, or if an appropriate data transfer mechanism (e.g., Standard Contractual Clauses) has been implemented. Without an appropriate transfer mechanism, data protection authorities may find EU to UK transfers in breach of the GDPR.

11.2 Please describe the mechanisms businesses typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).

When transferring personal data to a country other than an Adequate Jurisdiction, businesses must ensure that there are appropriate safeguards on the data transfer, as prescribed by the GDPR. The GDPR offers a number of ways to ensure compliance for international data transfers, of which one is consent of the relevant data subject. Other common options are the use of Standard Contractual Clauses or Binding Corporate Rules (“BCRs”).

Businesses can adopt the Standard Contractual Clauses drafted by the EU Commission – these are available for transfers between controllers, and transfers between a controller (as exporter) and a processor (as importer). International data transfers may also take place on the basis of contracts agreed between the data exporter and data importer provided that they conform to the protections outlined in the GDPR, and they have prior approval by the relevant data protection authority.

International data transfers within a group of businesses can be safeguarded by the implementation of BCRs. The BCRs will always need approval from the relevant data protection authority. Most importantly, the BCRs will need to include a mechanism to ensure they are legally binding and enforced by every member in the group of businesses. Among other things, the BCRs must set out the group structure of the businesses, the proposed data transfers and their purpose, the rights of data subjects, the mechanisms that will be implemented to ensure compliance with the GDPR and the relevant complainant procedures.

Transfer of personal data to the USA is also possible if the data importer has signed up to the EU-US Privacy Shield Framework, which was designed by the US Department of Commerce and the EU Commission to provide businesses in the EU and the US with a mechanism to comply with data protection requirements when transferring personal data from the EU to the US.

11.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.

It is likely that the international data transfer will require prior approval from the relevant data protection authority unless they have already established a GDPR-compliant mechanism, as set out above, for such transfers.

In any case, most of the safeguards outlined in the GDPR will need initial approval from the data protection authority, such as the establishment of BCRs.

12 Whistle-blower Hotlines

12.1 What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?

Internal whistle-blowing schemes are generally established in pursuance of a concern to implement proper corporate governance principles in the daily functioning of businesses. Whistle-blowing is designed as an additional mechanism for employees to report misconduct internally through a specific channel and supplements a business’s regular information and reporting channels, such as employee representatives, line management, quality-control personnel or internal auditors who are employed precisely to report such misconducts.
The WP29 has limited its Opinion 1/2006 on the application of EU data protection rules to internal whistle-blowing schemes to the fields of accounting, internal accounting controls, auditing matters, the fight against bribery, banking and financial crime. The scope of corporate whistle-blower hotlines, however, does not need to be limited to any particular issues. In the Opinion it is recommended that the business responsible for the whistle-blowing scheme should carefully assess whether it might be appropriate to limit the number of persons eligible for reporting alleged misconduct through the whistle-blowing scheme and whether it might be appropriate to limit the number of persons who may be reported through the scheme, in particular in the light of the seriousness of the alleged offences reported.

12.2 Is anonymous reporting prohibited, strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do businesses typically address this issue?

Anonymous reporting is not prohibited under EU data protection law; however, it raises problems as regards the essential requirement that personal data should only be collected fairly. In Opinion 1/2006, the WP29 considered that only identified reports should be advertised in order to satisfy this requirement. Businesses should not encourage or advertise the fact that anonymous reports may be made through a whistle-blower scheme.

An individual who intends to report to a whistle-blowing system should be aware that he/she will not suffer due to his/her action. The whistle-blower, at the time of establishing the first contact with the scheme, should be informed that his/her identity will be kept confidential at all stages of the process, and in particular will not be disclosed to third parties, such as the incriminated person or to the employee’s line management. If, despite this information, the person reporting to the scheme still wants to remain anonymous, the report will be accepted into the scheme. Whistle-blowers should be informed that their identity may need to be disclosed to the relevant people involved in any further investigation or subsequent judicial proceedings instigated as a result of any enquiry conducted by the whistle-blowing scheme.

13 CCTV

13.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?

A data protection impact assessment (“DPIA”) must be undertaken with assistance from the Data Protection Officer when there is a systematic monitoring of a publicly accessible area on a large scale. If the DPIA suggests that the processing would result in a high risk to the rights and freedoms of individuals prior to any action being taken by the controller, the controller must consult the data protection authority. During the course of a consultation, the controller must provide information on the responsibilities of the controller and/or processors involved, the purpose of the intended processing, a copy of the DPIA, the safeguards provided by the GDPR to protect the rights and freedoms of data subjects and, where applicable, the contact details of the Data Protection Officer.

If the data protection authority is of the opinion that the CCTV monitoring would infringe the GDPR, it has to provide written advice to the controller within eight weeks of the request of a consultation and can use any of its wider investigative, advisory and corrective powers outlined in the GDPR.

13.2 Are there limits on the purposes for which CCTV data may be used?

Personal data must be collected only for specified and legitimate purposes and must be used only in a manner which is not incompatible with the original purpose. For example, if a CCTV camera is used for the purpose of monitoring criminal activity in an office, it cannot later be used for a new and fundamentally different purpose (e.g., monitoring the work attendance of employees) without the provision of fresh notice to the affected individuals and, where appropriate, the obtaining of consent in advance.

14 Employee Monitoring

14.1 What types of employee monitoring are permitted (if any), and in what circumstances?

Employee monitoring must be lawful and fair. Employers must consider whether the monitoring methods are too intrusive, such that the employer’s legitimate interest is outweighed by the right to privacy. Employees must be notified of the extent of the monitoring prior to commencement, and why it is taking place.

14.2 Is consent or notice required? Describe how employers typically obtain consent or provide notice.

The GDPR requires a lawful basis for the monitoring of employees (e.g., consent or legitimate interests). However, consent is rarely used as it could easily be withheld or withdrawn by employees. In addition, because of the imbalance of power in the relationship between employer and employee, consent given in an employment context is unlikely to be deemed “freely given”, and therefore would not be valid. Generally, employers rely on the lawful basis of legitimate interests. This is subject to an assessment of proportionality and necessity. Employees must be given notice of the monitoring activities.

14.3 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?

As good practice, trade unions and employee representatives should be consulted where applicable.

15 Data Security and Data Breach

15.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?

Yes. Personal data must be processed in a way which ensures security and safeguards against unauthorised or unlawful processing, accidental loss, destruction and damage of the data. Both controllers and processors must ensure they have appropriate technical and organisational measures to meet the requirements of the GDPR. Depending on the security risk, this may include the...
encryption of personal data, the ability to ensure the ongoing confidentiality, integrity and resilience of processing systems, an ability to restore access to data following a technical or physical incident, and a process for regularly testing and evaluating the technical and organisational measures for ensuring the security of processing.

**16. Enforcement and Sanctions**

### 16.1 Describe the enforcement powers of the data protection authority(ies).  

<table>
<thead>
<tr>
<th>Investigatory Power</th>
<th>Civil/Administrative Sanction</th>
<th>Criminal Sanction</th>
</tr>
</thead>
<tbody>
<tr>
<td>Investigative</td>
<td>The data protection authority has wide powers to order the controller and the processor to provide any information it requires for the performance of its tasks, to conduct investigations in the form of data protection audits, to carry out review on certificates issued pursuant to the GDPR, to notify the controller or processor of alleged infringement of the GDPR, to access all personal data and all information necessary for the performance of controllers’ or processors’ tasks and access to the premises of the data including any data processing equipment.</td>
<td>N/A</td>
</tr>
<tr>
<td>Corrective</td>
<td>The data protection authority has a wide range of powers including to issue warnings or reprimands for non-compliance, to order the controller to disclose a personal data breach to the data subject, to impose a permanent or temporary ban on processing, to withdraw a certification and to impose an administrative fine (as below).</td>
<td>N/A</td>
</tr>
<tr>
<td>Authorisation</td>
<td>The data protection authority has a wide range of powers to advise the controller, accredit certification bodies and to authorise certificates, contractual clauses, administrative arrangements and BCRs as outlined in the GDPR.</td>
<td>N/A</td>
</tr>
<tr>
<td>Powers</td>
<td>The GDPR provides for administrative fines which can be €20 million or up to 4% of the business’ worldwide annual turnover of the proceeding financial year.</td>
<td>N/A</td>
</tr>
<tr>
<td>Imposition of</td>
<td>The GDPR provides for administrative fines which will be €20 million or up to 4% of the business’ worldwide annual turnover of the proceeding financial year, whichever is higher.</td>
<td>N/A</td>
</tr>
<tr>
<td>administrative</td>
<td>Non-compliance with a data protection authority</td>
<td></td>
</tr>
<tr>
<td>fines for</td>
<td></td>
<td></td>
</tr>
<tr>
<td>infringements of</td>
<td></td>
<td></td>
</tr>
<tr>
<td>specified GDPR</td>
<td></td>
<td></td>
</tr>
<tr>
<td>provisions</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### 16.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?

The GDPR entitles the relevant data protection authority to impose a temporary or definitive limitation, including a ban on processing.

### 16.3 Describe the data protection authority’s approach to exercising those powers, with examples of recent cases.

The ICO tends to co-operate with businesses before it takes enforcement action. Although unlikely, the ICO may take a different approach with respect to the enforcement of the GDPR.

---

**15.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.**

The controller is responsible for reporting a personal data breach without undue delay (and in any case within 72 hours of first becoming aware of the breach) to the relevant data protection authority, unless the breach is unlikely to result in a risk to the rights and freedoms of the data subject(s). A processor must notify any data breach to the controller without undue delay.

The notification must include the nature of the personal data breach, including the categories and number of data subjects concerned, the name and contact details of the Data Protection Officer or relevant point of contact, the likely consequences of the breach and the measures taken to address the breach, including attempts to mitigate possible adverse effects.

**15.3 Is there a legal requirement to report data breaches to affected data subjects? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.**

Controllers have a legal requirement to communicate the breach to the data subject, without undue delay, if the breach is likely to result in a high risk to the rights and freedoms of the data subject.

The notification must include the name and contact details of the Data Protection Officer (or point of contact), the likely consequences of the breach and any measures taken to remedy or mitigate the breach.

The controller may be exempt from notifying the data subject if the risk of harm is remote (e.g., because the affected data is encrypted), the controller has taken measures to minimise the risk of harm (e.g., suspending affected accounts) or the notification requires a disproportionate effort (e.g., a public notice of the breach).

**15.4 What are the maximum penalties for data security breaches?**

The maximum penalty is the higher of €20 million or 4% of worldwide turnover.
16.4 Does the data protection authority ever exercise its powers against businesses established in other jurisdictions? If so, how is this enforced?

The GDPR can also apply to non-EU businesses even if they have no physical presence in the EU (see the answer to question 3.1 above). Such businesses must appoint a representative in the EU against which the ICO or the relevant data protection authority can take relevant enforcement action under the GDPR.

17 E-discovery / Disclosure to Foreign Law Enforcement Agencies

17.1 How do businesses typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?

Most businesses will weigh the risks of non-compliance with the relevant foreign court order against the risks of non-compliance with the 2018 Act and determine which presents a lower risk. Assuming that the business decides to disclose the requested personal data, businesses will usually seek to justify such disclosures on the basis that they are necessary for the establishment, exercise or defence of legal claims.

17.2 What guidance has/have the data protection authority(ies) issued?

There is currently no standalone guidance from the ICO on this point under the DPA 2018.

18 Trends and Developments

18.1 What enforcement trends have emerged during the previous 12 months? Describe any relevant case law.

In 2018, the ICO issued a maximum possible fine of £500,000 under the DPA 1998 against a company for failing to protect the personal data of over 15 million people affected by the 2017 cyber attack on the credit reference agency. The GDPR allows for much higher fines, and it is expected that the ICO will issue these in the future.

18.2 What “hot topics” are currently a focus for the data protection regulator?

The largest single hot topic for the ICO at present is the impact of Brexit on transfers of personal data between the EU and the UK. While the outcome of the current discussions remains uncertain, the prospect of a “no deal” Brexit has forced many businesses to enter into Standard Contractual Clauses pre-emptively, to ensure that there is a valid transfer mechanism in place, in the event that the UK leaves the EU without an adequacy decision.
With one of the largest and most experienced data privacy and cybersecurity groups in the world, White & Case’s global team is on hand to guide clients through the relevant data protection legislation in the jurisdictions in which they are active. Seamlessly working with their counterparts in other practice areas, our global team has the depth of resources to provide integrated, creative and practical advice on the privacy-related concerns faced by our clients, wherever they are located.

Our experience spans the full range of industry sectors including financial institutions and banking, biotechnology, pharmaceuticals and chemicals, construction and engineering, consumer goods and retail, automotive, hotels and leisure, IT, telecommunications, manufacturing and electronics, publishing and media.

ATTORNEY ADVERTISING. Prior results do not guarantee a similar outcome. This publication is prepared for general information purposes only. It is not, and does not attempt to be, comprehensive in nature. Due to the general nature of its content, it should not be regarded as legal advice.
1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

There is no single principal data protection legislation in the United States. Rather, a jumble of hundreds of laws enacted on both the federal and state levels serve to protect the personal data of U.S. residents. At the federal level, the Federal Trade Commission Act (15 U.S. Code § 41 et seq.) broadly empowers the U.S. Federal Trade Commission (FTC) to bring enforcement actions to protect consumers against unfair or deceptive practices and to enforce federal privacy and data protection regulations. The FTC has taken the position that “deceptive practices” include a company’s failure to comply with its published privacy promises and its failure to provide adequate security of personal information, in addition to its use of deceptive advertising or marketing methods.

As described more fully below, other federal statutes primarily address specific sectors, such as financial services or healthcare. In parallel, state-level statutes protecting a wide range of privacy rights of individual residents, often differ considerably from one state to another, and cover areas as diverse as protecting library records to keeping home owners free from drone surveillance.

1.2 Is there any other general legislation that impacts data protection?

Although there is no general federal legislation, there are federal data protection laws which are typically sector-specific (see question 1.3 below) or focus on particular types of data. The Driver’s Privacy Protection Act of 1994 (DPPA) (18 U.S. Code § 2721 et seq.) governs the privacy and disclosure of personal information gathered by state Departments of Motor Vehicles, including photographs, Social Security Number (SSN), Driver Identification Number (DID), name, address (but not the five-digit ZIP code), telephone number, medical information and disability information. Children’s information is protected at the federal level under the Children’s Online Privacy Protection Act (COPPA) (15 U.S. Code § 6501), which prohibits the online collection of any information from a child under the age of 13, and requires publication of privacy notices and collection of verifiable parental consent when information from children is being collected. The Video Privacy Protection Act (VPPA) (18 U.S. Code § 2710 et seq.) was enacted to protect wrongful disclosure of videotape rental or sale records or similar audio-visual materials, including online streaming. Similarly, the Cable Communications Policy Act of 1984 includes provisions dedicated to the protection of subscriber privacy (47 U.S. Code § 551). The federal government and most states have enacted legislation that criminalises recording communications without obtaining consent from either one or all of the parties depending on the statute.

State laws also may impose restrictions and obligations on businesses relating to the collection, use, disclosure, security, or retention of special categories of information, such as biometric data, medical records, Social Security numbers, driver’s licence information, email addresses, library records, television viewing habits, financial records, tax records, insurance information, criminal justice information, phone records, and education records, just to name some of the most common. Similarly, states have enacted discrete laws pertaining to surveillance, including cellular location tracking, drone photography, and even smart TV “snooping” features.

Every state has adopted data breach notification legislation that applies to certain types of personal information about its residents. Even if a business does not have a physical presence in a particular state, it typically must comply with the state’s laws when faced with the unauthorised access to, or acquisition of, personal information it collects, holds, transfers or processes about that state’s residents. The types of information subject to these laws vary by state, with most defining personal information to include an individual’s first name or first initial and last name together with a data point including the individual’s Social Security Number, driver’s licence or state identification card number, financial account number or payment card information. Some states include additional triggering data points, such as date of birth, mother’s maiden name, passport number, biometric data, employee identification number or user name and password.

Some states are more active than others when it comes to data protection. Massachusetts, for example, has strong data protection regulations (201 CMR 1700) requiring any entity that holds, transmits or collects “personal information” of a Massachusetts resident to implement and maintain a comprehensive written data security plan addressing 12 designated activities. New York has adopted cybersecurity regulations (23 NYCRR 500) applicable to certain financial institutions doing business in the state, which set minimum standards and require companies to perform periodic risk assessments and file annual compliance certifications.

California has a long history of adopting privacy-forward legislation, and the state recently enacted the California Consumer Privacy Act (CCPA), which becomes effective on 1 January 2020. The law introduces new obligations on covered businesses, including requirements to disclose the categories of personal information the business collects about consumers, the specific pieces of personal information the business has collected about the consumer, the categories of sources from which the personal information is
collected, the business or commercial purpose for collecting or selling personal information, and the categories of third parties with which the business shares personal information. It also introduces new rights for California residents, including the right to request access to and deletion of personal information and the right to opt out of having personal information sold to third parties. The new requirements may force changes to data-driven business models and may necessitate significant updates to covered businesses’ external and internal privacy policies and operational compliance procedures.

1.3 Is there any sector-specific legislation that impacts data protection?

Key sector-specific laws include those covering financial services, healthcare, telecommunications, and education:

The Gramm Leach Bliley Act (GLBA) (15 U.S. Code § 6802(a) et seq.) governs the protection of personal information in the hands of banks, insurance companies and other companies in the financial service industry. This statute addresses “Non-Public Personal Information” (NPI), which includes any information that a financial service company collects from its customers in connection with the provision of its services. It imposes on financial service industry companies requirements for securing NPI, restricting disclosure and use of NPI and notifying customers when NPI is improperly exposed to unauthorised persons.

The Fair Credit Reporting Act (FCRA), as amended by Fair and Accurate Credit Transactions Act (FACTA) (15 U.S. Code § 1681), restricts use of information bearing on an individual’s creditworthiness, credit standing, credit capacity, character, general reputation, personal characteristics or mode of living to determine eligibility for credit, employment or insurance. It also requires truncating credit card numbers on printed receipts, requires certain types of personal information to be securely destroyed, and regulates the use of certain types of information received from affiliated companies for marketing purposes. Finally, it imposes obligations on financial institutions and creditors to institute programmes that detect and respond to instances of identity theft under its Identity Theft Red Flags Rule.

In addition to financial industry laws and regulation, the major credit card companies require businesses that process, store or transmit payment card data to comply with the Payment Card Industry Data Security Standard (PCI-DSS).

The Health Information Portability and Accountability Act, as amended (HIPAA) (29 U.S. Code § 1181 et seq.) protects information held by a covered entity that concerns health status, provision of healthcare or payment for healthcare that can be linked to an individual. Its Security Rule regulates the collection and disclosure of such information. Its Security Rule imposes requirements for securing this data.

The Telephone Consumer Protection Act (TCPA) (47 U.S. Code § 227) and associated regulations regulate calls and text messages to mobile phones and regulate calls to residential phones that are made for marketing purposes or using automated dialling systems or pre-recorded messages.

The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g) provides students with the right to inspect and revise their student records for accuracy, while also prohibiting the disclosure of these records or other personal information on the student, without the student’s or (in some instances) parent’s consent.

Where a federal statute covers a specific topic, the federal law may pre-empt any similar state law on that topic. However, certain federal laws, like GLBA for instance, specify that they are not pre-emptive of state laws on the subject.

1.4 What authority(ies) are responsible for data protection?

While the United States has no plenary data protection regulator, the FTC’s authority is very broad, and often sets the tone on federal privacy and data security issues. In addition, a variety of other agencies regulate data protection through sectoral laws, including the Office of the Comptroller of the Currency, the Department of Health and Human Services, the Federal Communications Commission, the Securities and Exchange Commission, the Consumer Financial Protection Bureau and the Department of Commerce.

2 Definitions

2.1 Please provide the key definitions used in the relevant legislation:

■ “Personal Data”

In the United States, information relating to an individual is typically referred to as “personal information” (rather than personal data). The definition of personal information in the U.S. is not uniform across all states or all regulations. In addition, certain data may be considered personal information for one purpose but not for another.

■ “Processing”

This is not applicable in our jurisdiction.

■ “Controller”

This is not applicable in our jurisdiction.

■ “Processor”

This is not applicable in our jurisdiction.

■ “Data Subject”

The state data protection statutes typically cover a “consumer” residing within the state. The definition of “consumer” differs by state. Under many state data protection statutes, a “consumer” is an individual who engages with a business for personal, family or household purposes. In contrast, under the newly enacted CCPA, a “consumer” is defined broadly as a “natural person who is a California resident”.

■ “Sensitive Personal Data”

This is not applicable in our jurisdiction.

■ “Data Breach”

The definition of a Data Breach depends on the individual state statute, but typically involves the unauthorised access or acquisition of computerised data that compromises the security, confidentiality, or integrity of personal information.

■ Other key definitions – please specify (e.g., “Pseudonymous Data”, “Direct Personal Data”, “Indirect Personal Data”) This is not applicable in our jurisdiction.

3 Territorial Scope

3.1 Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to those laws?

Businesses established in other jurisdictions may be subject to both federal and state data protection laws for activities impacting United States residents whose information the business collects, holds, transmits, processes or shares.
4 Key Principles

4.1 What are the key principles that apply to the processing of personal data?

- **Transparency**
  The FTC has issued guidelines espousing the principle of transparency, recommending that businesses: (i) provide clearer, shorter, and more standardised privacy notices that enable consumers to better comprehend privacy practices; (ii) provide reasonable access to the consumer data they maintain that is proportionate to the sensitivity of the data and the nature of its use; and (iii) expand efforts to educate consumers about commercial data privacy practices.

- **Lawful basis for processing**
  While there is no “lawful basis for processing” requirement under U.S. law, the FTC recommends that businesses provide notice to consumers of their data collection, use and sharing practices and obtain consent in limited circumstances where the use of consumer data is materially different than claimed when the data was collected, or where sensitive data is collected for certain purposes.

- **Purpose limitation**
  The FTC recommends privacy-by-design practices that include limiting “data collection to that which is consistent with the context of a particular transaction or the consumer’s relationship with the business, or as required or specifically authorized by law”.

- **Data minimisation**
  See above.

- **Proportionality**
  See above.

- **Retention**
  The FTC recommends privacy-by-design practices that implement “reasonable restrictions on the retention of data”, including disposal “once the data has outlived the legitimate purpose for which it was collected”.

- **Other key principles – please specify**
  This is not applicable in our jurisdiction.

5 Individual Rights

5.1 What are the key rights that individuals have in relation to the processing of their personal data?

- **Right of access to data/copies of data**
  These rights are statute-specific. For example, under certain circumstances, employees are entitled to receive copies of data held by employers. In other circumstances, parents are entitled to receive copies of information collected online from their children under the age of 13. Under HIPAA, individuals are entitled to request copies of medical information held by a health services provider. Further, under the FCRA, individuals are permitted to receive a copy of consumer report information that is maintained by a consumer reporting agency. In addition, the CCPA provides a right of access for California residents to personal information held by a business relating to that resident.

- **Right to rectification of errors**
  These rights are statute-specific. Some laws, such as the FCRA, provide consumers with a right to review data about the consumer held by an entity and request corrections to errors in that data. At the state level, the right to correct information commonly attaches to credit reports, as well as criminal justice information, employment records, and medical records.

- **Right to deletion**
  These rights are statute-specific. By way of a federal law example, COPPA provides parents the right to review and delete their children’s information and may require that data be deleted even in the absence of a request. Some state laws, such as the CCPA, provide a right of deletion for California residents, with certain exceptions.

- **Right to object to processing**
  These rights are statute-specific. Individuals are given the right to opt out of receiving commercial (advertising) emails under CAN-SPAM and the right to not receive certain types of calls to residential or mobile telephone numbers without express consent under the TCPA. Some states provide individuals with the right not to have telephone calls recorded without either the consent of all parties to the call or the consent of one party to the call.

- **Right to restrict processing**
  These rights are statute-specific. Certain laws restrict how an entity may process consumer data. For example, the CCPA allows California residents to prohibit a business from selling that individual’s personal information.

- **Right to data portability**
  These rights are statute-specific. Examples of consumer rights to data portability exist under HIPAA, where individuals are entitled to request that medical information held by a health services provider be transferred to another health services provider. In addition, the CCPA provides a right of data portability for California residents.

- **Right to withdraw consent**
  These rights are statute-specific. By way of example, under the TCPA, individuals are permitted to withdraw consent given to receive certain types of calls to residential or mobile telephone lines.

- **Right to object to marketing**
  These rights are statute-specific. Several laws permit consumers to restrict marketing activities involving their personal data. Under CAN-SPAM, for example, individuals may opt out of receiving commercial (advertising) emails. Under the TCPA, individuals must provide express written consent to receive marketing calls/texts to mobile telephone lines. California’s Shine the Light Act requires companies that share personal information for the recipient’s direct marketing purposes to either provide an opt-out or make certain disclosures to the consumer of what information is shared, and with whom.

- **Right to complain to the relevant data protection authority(ies)**
  These rights are statute-specific. By way of example, individuals may report unwanted or deceptive commercial email (“spam”) directly to the FTC, and telemarketing violations directly to the Federal Communications Commission (FCC). Similarly, anyone may file a HIPAA complaint directly with the Department of Health and Human Services (HHS). At the state level, California residents may report alleged violations of the CCPA to the California Attorney General.

- **Other key rights – please specify**
  This is not applicable in our jurisdiction.
### 6 Registration Formalities and Prior Approval

#### 6.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?

No, there is no such obligation.

#### 6.2 If such registration/notification is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?

This is not applicable in our jurisdiction.

#### 6.3 On what basis are registrations/notifications made (e.g., per legal entity, per processing purpose, per data category, per system or database)?

This is not applicable in our jurisdiction.

#### 6.4 Who must register with/notify the data protection authority (e.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation)?

This is not applicable in our jurisdiction.

#### 6.5 What information must be included in the registration/notification (e.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes)?

This is not applicable in our jurisdiction.

#### 6.6 What are the sanctions for failure to register/notify where required?

This is not applicable in our jurisdiction.

#### 6.7 What is the fee per registration/notification (if applicable)?

This is not applicable in our jurisdiction.

#### 6.8 How frequently must registrations/notifications be renewed (if applicable)?

This is not applicable in our jurisdiction.

#### 6.9 Is any prior approval required from the data protection regulator?

This is not applicable in our jurisdiction.

#### 6.10 Can the registration/notifications be completed online?

This is not applicable in our jurisdiction.

#### 6.11 Is there a publicly available list of completed registrations/notifications?

This is not applicable in our jurisdiction.

#### 6.12 How long does a typical registration/notification process take?

This is not applicable in our jurisdiction.

### 7 Appointment of a Data Protection Officer

#### 7.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.

Appointment of a Data Protection Officer is not required under U.S. law, but certain statutes require the appointment or designation of an individual or individuals who are charged with compliance with the privacy and data security requirements under the statute. These include GLBA, HIPAA, and the Massachusetts Data Security Regulation, for example.

#### 7.2 What are the sanctions for failing to appoint a Data Protection Officer where required?

Potential sanctions are statute/regulator-specific.

#### 7.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect to his or her role as a Data Protection Officer?

This is not applicable in our jurisdiction.

#### 7.4 Can a business appoint a single Data Protection Officer to cover multiple entities?

This is not applicable in our jurisdiction.

#### 7.5 Please describe any specific qualifications for the Data Protection Officer required by law.

This is not applicable in our jurisdiction.

#### 7.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?

This is not applicable in our jurisdiction.
**7.7 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?**

This is not applicable in our jurisdiction.

**7.8 Must the Data Protection Officer be named in a publicly-facing privacy notice or equivalent document?**

This is not applicable in our jurisdiction.

---

**8 Appointment of Processors**

**8.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?**

Under certain state laws and federal regulatory guidance, if a business shares certain categories of personal information with a vendor, the business is required to contractually bind the vendor to reasonable security practices. HIPAA, for example, requires the use of Business Associate Agreements for the transfer of protected health information to vendors.

**8.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?**

The form of the contract typically is not specified. HIPAA, however, is an example of a statute with minimum requirements for provisions that must be included within Business Associate Agreements. These agreements must include limitations on use and disclosure, and require vendors to abide by HIPAA’s Security Rule, to provide breach notification and report on unauthorised use and disclosure, to return or destroy protected data, and to make its books, records, and practices available to the federal regulator.

---

**9 Marketing**

**9.1 Please describe any legislative restrictions on the sending of electronic direct marketing (e.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?).**

Prior express consent is required under the TCPA before certain marketing texts may be sent to a mobile telephone line. Other federal statutes have opt-out rather than opt-in consent requirements. For instance, under CAN-SPAM, marketing emails – or emails sent for the primary purpose of advertising or promoting a commercial product or service – may be sent to those not opting out, provided the sender is accurately identified, the subject line and text of the email are not deceptive, the email contains the name and address of the sender, the email contains a free, simple mechanism to opt out of future emails, and the sender honours opt-outs within 10 days of receipt.

**9.2 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.).**

Marketing by telephone is regulated on the national level by the Telemarketing Sales Rule, a regulation under the Telemarketing and Consumer Fraud and Abuse Prevention Act. This act established the national Do-Not-Call list of telephone numbers that cannot be used for marketing communications (calls and texts) and disclosure requirements for companies engaging in telephone marketing. It also sets limitations on the use of telephone marketing, including, for instance, limiting the time of day for marketing calls, requiring the caller to provide an opt-out of future calls, and limiting the use of pre-recorded messages. There are no consent or opt-out requirements for sending marketing materials through postal mail.

It is noted that the Federal Trade Commission, which regulates deceptive practices, has brought enforcement actions relating to the transmission of marketing emails or telemarketing calls by companies who have made promises in their publicly posted privacy policies that personal information will not be used for marketing purposes. Additionally, many states apply “deceptive practices” statutes to impose penalties or injunctive relief in similar circumstances, or where violation of a federal statute is deemed a deceptive practice under state law.

**9.3 Do the restrictions noted above apply to marketing sent from other jurisdictions?**

Yes, if the recipient is within the United States.

**9.4 Is/are the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?**

The FTC, FCC, and the Attorneys General of the states are active in enforcement in this area.

**9.5 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?**

Yes; however, the purchaser of the list should scrub it against the national Do-Not-Call list and the purchaser’s email opt-out lists. Some states forbid the sale of email addresses of individuals who have opted out of receiving marketing emails and some forbid the sale of information obtained in connection with a consumer’s purchase transaction.

**9.6 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?**

The penalties under CAN-SPAM can range from US$16,000 to US$41,484 per email. The penalties under the Telephone Consumer Protection Act can reach up to US$16,000 for each text message or call sent in violation of the Act for certain entities. By way of example, the FTC and the Attorneys General of several states obtained a judgment of US$280 million in 2017 for violation of the Telephone Consumer Protection Act., the FTC’s Telemarketing Sales Rule, and state law.
Many states have their own “deceptive practices” statutes which impose additional state penalties where violations of federal statutes are deemed to be deceptive practices under the state statute.

10 Cookies

10.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).

The federal Computer Fraud and Abuse Act has been used to assert legal claims against the use of cookies for behavioural advertising, where the cookies enable deep packet inspection of the computer on which they are placed. At least two states, California and Delaware, require disclosures to be made where cookies are used to collect information about a consumer’s online activities across different websites or over time. The required disclosure must include how the operator responds to so-called “do not track” signals or other similar mechanisms.

In addition, the FTC Act and state “deceptive practices” acts have underpinned regulatory enforcement and private class action lawsuits against companies that failed to disclose or misrepresented their use of tracking cookies. One company settled an action in 2012 with a payment of US$22.5 million to the FTC, and in 2016 agreed to pay US$5.5 million to settle a private class action involving the same conduct.

10.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?

The Computer Fraud and Abuse Act and the Electronic Communications Privacy, as well as state surveillance laws, may come into play where cookies collect information from the computer on which they are placed and report that information to the entity placing the cookies without proper consent.

10.3 To date, has/have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?

Yes, the FTC has brought regulatory enforcement actions against companies that failed to disclose or misrepresented their use of cookies.

10.4 What are the maximum penalties for breaches of applicable cookie restrictions?

Maximum fines are not set by statute.

11 Restrictions on International Data Transfers

11.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.

The U.S. does not place restrictions on the transfer of personal data to other jurisdictions.

11.2 Please describe the mechanisms businesses typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).

This is left to the discretion of the company, as the U.S. does not place restrictions on the transfer of personal data to other jurisdictions. With respect to receiving data from abroad, the EU-U.S. Privacy Shield Framework provides a mechanism to comply with data protection requirements when transferring personal data from the European Union to the United States.

11.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.

This is not required in our jurisdiction.

12 Whistle-blower Hotlines

12.1 What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?

The federal Whistleblower Protection Act of 1989 protects federal employees, and some states have similar statutes protecting state employees. Public companies subject to the Sarbanes-Oxley Act also are required to have a Whistleblower policy which must be approved by the board of directors and create a procedure for receiving complaints from whistleblowers.

12.2 Is anonymous reporting prohibited, strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do businesses typically address this issue?

Anonymous reporting generally is permitted. Rule 10A-3 of the Securities Exchange Act of 1934, for example, requires that audit committees of publicly listed companies establish procedures for the confidential, anonymous submission by employees of concerns regarding questionable accounting or auditing matters.

13 CCTV

13.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?

The use of CCTV must comply with federal and state criminal voyeurism/eavesdropping statutes, some of which require posting signs where video monitoring is taking place, restrict the use of hidden cameras, or prohibit videotaping altogether if the location is
13.2 Are there limits on the purposes for which CCTV data may be used?

There generally are no restrictions on the use of lawfully collected CCTV data, subject to a company’s own stated policies or labour agreements.

14 Employee Monitoring

14.1 What types of employee monitoring are permitted (if any), and in what circumstances?

Employee privacy rights, like those of any individual, are based on the principle that an individual has an expectation of privacy unless that expectation has been diminished or eliminated by context, agreement, notice, or statute. Monitoring of employees generally is permitted to the same extent as it is with the public, including when the employer makes clear disclosure regarding the type and scope of monitoring in which it engages, and subject to generally applicable surveillance laws regarding inherently private locations as well as employee-specific laws, such as those regarding the privacy of union member activities.

14.2 Is consent or notice required? Describe how employers typically obtain consent or provide notice.

Consent and notice rights are state-specific, as is the use of hidden cameras. When required or voluntarily obtained, employers typically obtain consent for employee monitoring through the acceptance of employee handbooks, and may provide notice by appropriately posting signs.

14.3 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?

The National Labor Relations Act prohibits employers from monitoring their employees while they are engaged in protected union activities.

15 Data Security and Data Breach

15.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?

In the consumer context, the FTC has stated that a company’s data security measures for protecting personal data must be “reasonable”, taking into account numerous factors, to include the volume and sensitivity of information the company holds, the size and complexity of the company’s operations, and the cost of the tools that are available to address vulnerabilities. Certain federal statutes and certain individual state statutes also impose an obligation to ensure the security of personal information. For example, GLBA and HIPAA impose security requirements on financial services and covered healthcare entities (and their vendors). Some states impose data security obligations on certain entities that collect, hold or transmit limited types of personal information. For example, the New York Department of Financial Services (NYDFS) adopted regulations in 2017 that obligate all “regulated entities” to adopt a cybersecurity programme and cybersecurity governance processes. The regulations also mandate the reporting of cybersecurity events, like data breaches and attempted infiltrations, to regulators. Covered entities include those banks, mortgage companies, insurance companies, and check-cashers otherwise regulated by the NYDFS.

15.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expects voluntary breach reporting.

At the federal level, other than breach notification requirements pertaining to federal agencies themselves, HIPAA requires a “Covered Entity” to report an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information to the Department of Health and Human Services. If the breach involves more than 500 individuals, such notification must be made within 60 days of discovery of the breach. Information to be submitted includes information about the entity suffering the breach, the nature of the breach, the timing (start and end) of the breach, the timing of discovery of the breach, the type of information exposed, safeguards in place prior to the breach, and actions taken following the breach, including notifications sent to impacted individuals and remedial actions.

While not specifically a data breach notification obligation, the Securities and Exchange Act and associated regulations, including Regulation S-K, require public companies to disclose in filings with the Securities and Exchange Commission when material events, including cyber incidents, occur. Registrants are required to disclose conclusions on the effectiveness of disclosure controls and procedures. To the extent cyber incidents pose a risk to a registrant’s ability to record, process, summarise and report information that is required to be disclosed in SEC Commission filings, management should also consider whether there are any deficiencies in its disclosure controls and procedures that would render them ineffective.

Some state statutes require the reporting of data breaches to a state agency or Attorney General under certain conditions. The information to be submitted varies by state but generally includes a description of the incident, the number of individuals impacted, the types of information exposed, the timing of the incident and the discovery, actions taken to prevent future occurrences, copies of notices sent to impacted individuals, and any services offered to impacted individuals, such as credit monitoring.

15.3 Is there a legal requirement to report data breaches to affected data subjects? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

At the federal level, HIPAA requires covered entities to report data breaches to impacted individuals without unreasonable delay, and in no case later than 60 days. Notice should include a description of the breach, to include: the types of information that were involved; the steps individuals should take to protect themselves, including who they can contact at the covered entity for more information; as well as the measures being taken to prevent future breaches. Some states require notification to be in writing. The Federal Trade Commission (FTC) requires data breach notices to include the name and contact information of the organisation, the type of data involved, and whether more steps need to be taken to protect consumers.
15.4 What are the maximum penalties for data security breaches?

Penalties are statute- and fact-specific. Under HIPAA, for example, fines can range from US$100 to US$50,000 per violation (or per record), with a maximum penalty of US$1.5 million per year for each violation. In 2018, a company paid a record penalty of US$148 million in a data breach settlement reached with all 50 states and the District of Columbia.

16 Enforcement and Sanctions

16.1 Describe the enforcement powers of the data protection authority(ies).

Please see questions 16.2 to 16.4 below.

16.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?

The U.S. does not have a central data protection authority. Enforcement authority is specified in the relevant statutes. Some include only federal government enforcement, some allow for federal or state government enforcement, and some allow for enforcement through a private right of action by aggrieved consumers. Whether the sanctions are civil and/or criminal depends on the relevant statute.

16.3 Describe the data protection authority’s approach to exercising those powers, with examples of recent cases.

In the U.S., this depends on the relevant statutory enforcement mechanism and the agency conducting the enforcement measures. The FTC, for example, published a guide in 2015 that offered 10 practical lessons businesses can learn from its review of over 50 FTC data security enforcement action settlements.

16.4 Does the data protection authority ever exercise its powers against businesses established in other jurisdictions? If so, how is this enforced?

Extraterritorial enforcement of a U.S. law would depend on a number of factors, including whether the entity is subject to the jurisdiction of the U.S. courts, the impact on U.S. commerce and the impact on U.S. residents, among other factors.

17 E-discovery / Disclosure to Foreign Law Enforcement Agencies

17.1 How do businesses typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?

When made pursuant to Mutual Legal Assistance Treaties, information requests are typically processed through the DOJ, which works with the local U.S. Attorney’s Office and local law enforcement, prior to review by a federal judge and service on the U.S. company.

17.2 What guidance has/have the data protection authority(ies) issued?

Guidance is agency-specific, and there is no central data protection authority. By way of example, the FTC has issued guidance on a variety of issues, including children’s privacy, identity theft and telemarketing. Some state Attorneys General have also offered resources on their websites for victims of identity theft and for companies suffering data security breaches.

18 Trends and Developments

18.1 What enforcement trends have emerged during the previous 12 months? Describe any relevant case law.

The FTC remains active in regulating data security and privacy issues, despite having suffered a rare federal appellate court loss in 2018. The court found the FTC inappropriately required a medical lab company “to overhaul and replace its data security program to meet an indeterminable standard of reasonableness”, following an alleged data breach. Because the FTC order failed to enjoin any specific act or practice, the court held that the cease-and-desist order was unenforceable.

In early 2018, the FTC brought its first children’s privacy action involving connected toys. The FTC alleged that a toymaker violated COPPA by collecting personal information from children without notice or parental consent, by failing to take reasonable steps to
secure the collected data it collected, and by falsely stating in its privacy policy that personal information obtained through its platforms would be encrypted. In addition to paying a monetary settlement of US$650,000, the toymaker must implement a comprehensive data security programme, which will be subject to independent audits for 20 years.

HHS remains active in enforcing HIPAA violations, imposing its largest ever fine to date in 2018 – US$16 million – following a series of alleged cyber-attacks on a health insurer. In early 2019, the regulator obtained a US$3 million settlement against a not-for-profit hospital system that suffered from two data breaches, and whose non-compliance included its failure to conduct a comprehensive risk analysis, failure to implement sufficient security measures, and failure to obtain a written Business Associate Agreement with a vendor that maintained electronic protected health information on its behalf.

State Attorneys General also play a key role in bringing enforcement actions under specific state laws. For example, in late 2018, the D.C. Attorney General sued a social media company alleging that the company improperly allowed a third party to gain access to information on D.C. residents for use in targeted political ad campaigns. Finally, private litigants commonly file class action civil lawsuits in the United States following any major personal data breach.

The FTC is undertaking a re-examination of its approach to consumer privacy, which is its first comprehensive review of the area since 2012. The results of the FTC’s review likely will dictate future enforcement priorities and rulemaking. The FTC kicked off 2019 focused on the privacy practices of broadband providers, having issued orders to seven U.S. internet providers demanding responses about the categories of personal information they collect about consumers and their devices, and what processes and techniques the companies use to the extent they aggregate, anonymise or de-identify data.

At the state level, insurance commissioners are increasing their attention to data protection and systems security, with the South Carolina Insurance Data Security Act leading a likely trend for the industry to be governed by laws that mirror the National Association of Insurance Commissioners (NAIC) Data Security Model Law.

Steven Chabinsky is the global chair of White & Case’s international Data, Privacy & Cybersecurity legal practice. Steve advises multinational clients across industries on a broad range of data protection, cybersecurity risk management, and data breach response matters.

Prior to joining White & Case, Steve served as General Counsel and Chief Risk Officer for the international cybersecurity technology firm CrowdStrike, and in 2016 was Presidentially appointed as a Commissioner on the nonpartisan White House Commission on Enhancing National Cybersecurity. Steve’s prior government service is extensive, and includes his having served as Deputy Assistant Director of the FBI’s Cyber Division, after having organised and led the Bureau’s Cyber Intelligence programme and served as the FBI’s top cyber lawyer.

Steve received his undergraduate and law degrees from Duke University.

F. Paul Pittman is an associate in White & Case’s international Data, Privacy & Cybersecurity legal practice. Paul advises clients on the complex issues that often arise in the handling of consumer and business data, and in the management of information and operational systems under state, federal and international laws and standards.

Paul’s practice includes guiding companies in responding to data breaches, identifying and helping clients resolve data privacy and cybersecurity issues in business operations and products, including connected devices (IoT), and assisting clients with the development of compliant data privacy and cybersecurity programmes. In addition, Paul counsels clients on the permissible handling of data consistent with online and mobile standards. Paul also advises global clients on all data privacy and cybersecurity matters that arise in corporate transactions.

Paul received a Bachelor of Science degree from Allegheny College, and a Juris Doctor degree from Washington and Lee University School of Law.

**18.2 What “hot topics” are currently a focus for the data protection regulator?**

With one of the largest and most experienced data privacy and cybersecurity groups in the world, White & Case's global team is on hand to guide clients through the relevant data protection legislation in the jurisdictions in which they are active. Seamlessly working with their counterparts in other practice areas, our global team has the depth of resources to provide integrated, creative and practical advice on the privacy-related concerns faced by our clients, wherever they are located.

Our experience spans the full range of industry sectors including financial institutions and banking, biotechnology, pharmaceuticals and chemicals, construction and engineering, consumer goods and retail, automotive, hotels and leisure, IT, telecommunications, manufacturing and electronics, publishing and media.

© Published and reproduced with kind permission by Global Legal Group Ltd, London
Current titles in the ICLG series include:

- Alternative Investment Funds
- Anti-Money Laundering
- Aviation Law
- Business Crime
- Cartels & Leniency
- Class & Group Actions
- Competition Litigation
- Construction & Engineering Law
- Copyright
- Corporate Governance
- Corporate Immigration
- Corporate Investigations
- Corporate Recovery & Insolvency
- Corporate Tax
- Cybersecurity
- Data Protection
- Employment & Labour Law
- Enforcement of Foreign Judgments
- Environment & Climate Change Law
- Family Law
- Financial Services Disputes
- Fintech
- Franchise
- Gambling
- Insurance & Reinsurance
- International Arbitration
- Investor-State Arbitration
- Lending & Secured Finance
- Litigation & Dispute Resolution
- Merger Control
- Mergers & Acquisitions
- Mining Law
- Oil & Gas Regulation
- Outsourcing
- Patents
- Pharmaceutical Advertising
- Private Client
- Private Equity
- Product Liability
- Project Finance
- Public Investment Funds
- Public Procurement
- Real Estate
- Securitisation
- Shipping Law
- Telecoms, Media & Internet
- Trade Marks
- Vertical Agreements and Dominant Firms