# Table of Contents

**INTRODUCTION**  
1

**Americas**  
2  
Argentina  
3  
Brazil  
6  
Canada  
8  
Colombia  
10  
Mexico  
12  
United States  
14  
Venezuela  
16

**EMEA**  
19  
Austria  
20  
Belgium  
21  
Czech Republic  
23  
Denmark  
25  
Finland  
26  
France  
27  
Germany  
30  
Greece  
33  
Hungary  
35  
Ireland  
38  
Italy  
41  
Netherlands  
43  
Norway  
46  
Poland  
47  
Portugal  
48  
Slovakia  
49  
Spain  
50  
Sweden  
53  
Switzerland  
55  
United Kingdom  
58
Asia Pacific
Australia  60
China (PRC)  61
Hong Kong  65
Indonesia  67
Japan  68
Malaysia  70
Philippines  71
Singapore  73
South Korea  74
Taiwan  78
About Our Practice  80
INTRODUCTION

Nearly every company in the world is struggling to effectively manage the broad range of legal and operational risks associated with data. Data is everywhere, and everyone is working to avoid wrongful disclosures, theft of informational assets, and the losses related to the costly legal fallout. This is the result, in large part, of the heightened regulatory scrutiny and marketplace expectations facing multinationals linked electronically across country borders, and increasingly dependent on service providers for their core business functions.

Against this backdrop, Baker & McKenzie is pleased to present the results of its Global Data Protection Enforcement Report. We set out to give legal and compliance risk managers an understanding of the data enforcement laws in place around the world in the hopes of better equipping them to make informed decisions about how to manage risks associated with data. To this end, we surveyed local counsel in 37 jurisdictions throughout the Americas, EMEA, and APAC, and asked them to describe the legal risks associated with violations of data protection laws, and summarize enforcement activities among local data protection authorities.

The findings of this Report further demonstrate how important it is to enhance compliance controls in large, multinational corporations with the goal of reducing the risk of an enforcement action on foreign soil. These internal compliance controls include conducting Privacy Impact Assessments, preparing data flow maps as part of any new project involving cross-border data transfers, and creating a culture of awareness surrounding privacy and the wide spectrum of potentially applicable laws. We hope you find it useful within your organizations.

About Baker & McKenzie

Baker & McKenzie is a global law firm with more than 4,200 lawyers in 47 countries. We routinely help global enterprises with a vast array of privacy and data security compliance issues, from core compliance steps for the processing of customer and employee personal data, to more complex issues such as system and employee monitoring, cross border transfer vehicles, security breach notice and response, and global CRM implementations. We also help companies address privacy issues that arise in the context of internal investigations and transactions, responding to data access requests, and conducting multi-jurisdictional surveys. We frequently advise clients on implementing enterprise-wide privacy programs, and help clients track progress via privacy maturity models and other measurement tools. We provide a holistic approach to managing business information by implementing processes, roles, controls and metrics that treat information as a valuable resource.
Americas
Argentina

Administrative Remedies

The Argentine Personal Data Protection Authority (the “Authority”) has the power, among other things, to conduct inspections/audits; investigate complaints and cases; apply administrative sanctions; act as a private plaintiff (“querellante”) in criminal proceedings initiated as a consequence of breaches to Argentine Personal Data Protection Law No. 25,326 and its related regulations (the “Law”); order the registration of databases, the suspension of processing and/or transfer of personal data, and other similar actions; these orders can be eventually appealed to local courts.

In addition to the Law, the 1996 Confidentiality Law No. 24,766, punishes anyone that uses or reveals secret information that has a commercial value and has been reasonably protected.

The Law provides that the owner of such confidential information may avoid that:

☑ Such information is disclosed to third parties without the owner’s previous consent; or
☑ Is used by third parties in violation of accepted commercial practices (such as the breach of contractual obligations, the abuse of confidence, etc.).

In order to ensure this, the confidential information (the “Information”):

☑ Shall be secret (the information is not generally available for the public or has limited access);
☑ has a commercial value due to its secret status; and
☑ The owner has adopted reasonable measures to protect it.

The Law sets forth that any person who has access to the Information for the purpose of his/her work, job title, profession or business relation, and provided that he/she was made aware of the confidentiality of such Information, shall abstain from disclosing such Information without any justified cause or authorization. The Law states that its provisions are applicable to any Information contained in paper, electronic or magnetic form, optic discs, and microfilms and/or films. To protect such Information, the law provides certain legal remedies for its owner, for instance preliminary injunctions, civil actions to prohibit the use of such confidential information by a third party and/or compensation for damages.

Civil Remedies

Individuals may file complaints with the Authority, and can seek indemnification and judicial remedies for damages suffered as a consequence of breaches of the Law.

Please note that the provisions of the Law are relevant, as they apply as public policy (“orden público”) and cannot be waived by data owners or processors of personal data.
Criminal Remedies

The Law has amended the Argentine Criminal Code (the “Code”). In this regard, the Code considers it a criminal offense to knowingly process false personal data and to breach confidentiality or data security measures in order to access databases. In this sense, the Code provides for imprisonment penalties ranging between 3 to 6 years (or 4 ½ years to 9 years in case of harm to any individual), and disqualification from holding any public office for civil servants.

As regards privacy violations, the Code provides for:

(i) Imprisonment penalties ranging from 15 days to 6 months, which apply for opening electronic communications or letters; or intercepting electronic communications or telephone calls;

(ii) For imprisonment penalties ranging from 1 month to 1 year, if the individual that breaches the law communicates the content to someone else and/or publishes the content of the letter, etc.;

(iii) Imprisonment penalties ranging from 1 month to 2 years, for gaining access to a database by violating confidential and security systems; providing or revealing confidential information registered in a database; inputting or forcing another to input false data into a database; and

(iv) Additional sanctions apply in all cases above mentioned if the individual that breaches the law is a public officer.

Finally, fines are also contemplated in the Code under certain cases.

Other Remedies

The Authority may impose the following administrative sanctions:

(i) Warnings;

(ii) Suspension;

(iii) Fines ranging between AR$1,000 and AR$100,000; and

(iv) Closure or cancellation of the file, register or databases.

Disposition No. 9/2015 issued by the Authority distinguishes three categories of infringement (“Low infringements”, “Critical Infringements”, “Very Critical Infringements”) to determine the graduation of the administrative sanctions to be applied to each particular case. In this regard, “Low infringements” are penalized with fines ranging between AR$1,000 and AR$25,000; “Critical Infringements” are penalized with fines that range between AR$25,001 and AR$80,000 and an suspension of the file for a period of up to 30 days; and “Very Critical Infringements” are penalized with fines ranging between AR$80,001 and AR$100,000 and an suspension of the file for a period of a minimum of 31 days to a maximum of 365 days and/or cancelation of the file. The category of each infringement would depend on the circumstances of each case.

Due to the fluctuation of the exchange rate, we usually suggest that the amount of any fine in US$ be calculated once the same is imposed and is in effect (meaning that no decision of any appeal is still pending).
It is important to highlight that the Authority is actively conducting audits to confirm if processors of personal data comply with security obligations and registration of databases (for instance, human resources databases).

While the Authority may impose the previously mentioned sanctions, at the moment these sanctions tend to be only warnings and are directed to rectify processors’ future practices. However, fines would probably be imposed by the Authority to processors who do not rectify their practices after being subject to an audit and/or requirement from the Authority.

In any event, please note that the Authority keeps a registry of the sanctions imposed to data processors. As per the information provided by the Authority, most sanctions imposed since 2007 have been warnings. In relation to the fines imposed by the Authority, most of the fines have been categorized as "Low Infringements" (as per the categorization resulting from Disposition No. 9/2015 previously mentioned) with an average value of AR$3,000. Notwithstanding the foregoing, the Authority has applied fines categorized as "Critical Infringements" and "Very Critical Infringements" for an amount ranging from AR$40,000 to AR$60,000.

Additionally, there are a limited number of published legal precedents in which local courts have ordered the indemnification of data owners in amounts ranging between AR$1,000 and AR$25,000, for damages suffered by data owners due to registration of inaccurate/false data in financial databases.

Further examples of cases of enforcement action in Argentina include:

- In April 2007, fines were imposed on Banco Galicia, Bank of Boston and Banco Patagonia in “Sánchez Miguel Ángel c/Banco de Galicia y Buenos Aires y otros s/daños y perjuicios” - CNCIV - Sala B;
- On March 4, 2003, a fine was imposed on the Central Bank in “Gutiérrez, Norma Susana c/ BCRA y Otro “ - CNApel. CCFed; and
- On February 6, 2002 a fine was imposed in "Ravina, Arturo Octavio c/ Organización Veraz S.A.", CNCiv., Sala F.
Brazil

Administrative Remedies

None. There is no agency in Brazil specialized in verifying compliance with data protection rules. However, the new government may propose this year a bill of law that will deal specifically with data protection and its compliance in Brazil.

Civil Remedies

Indians can bring claims for actual as well as moral damages.

In case of violation of data protection rules established in the Internet Legal Framework, civil sanctions can vary from: (a) warnings, (b) fines in the amount of up to 10% of the economic group’s (to which the company that has violated the rule belongs to) revenues in Brazil in the last year, (c) temporary suspension of data collection activities or (d) prohibition of data collection activities. Please see below in general comments for more detailed information on the Internet Legal Framework. As such Law has been recently enacted, some provisions are yet to be regulated by the government.

Besides, a violation of any data protection rule established in the Consumer Defense Code, as further explained below, can be penalized with fines up to R$ 6.000.000. Such penalties may be imposed by specialized agencies entitled to "defend" consumers’ rights broadly ("PROCONs") or the Consumer District Attorney's Office. Administrative procedures as such have been conducted by authorities, but in a confidential basis which prevent us from having further details about them.

Criminal Remedies

Potential criminal liability for unauthorized interceptions of electronic communications (subject to imprisonment from 2 to 4 years, plus fines) and other specific matters.

In addition, depending on the nature of the data (e.g. banking, tax), unauthorized access or breaches also constitute a crime (subject to imprisonment from 1 to 4 years, plus fines).

There is also criminal liability for accessing computer devices to obtain information without the computer owner’s authorization (subject to imprisonment from 3 months to 1 year, plus fines, and such penalty might be increased up to 1/3 if the breach caused economic damage).

The penalty shall be increased if the information obtained consists of private electronic communications, confidential information or trade secrets (subject to imprisonment from 6 months to 2 years, plus a fine if no greater offence was committed).

If a greater offence was committed, e.g. if confidential information is obtained by breaching a computer device and a fraud is committed by using such information, such individual shall be subject to imprisonment from 1 to 5 years, plus fine (which is the penalty applicable for fraud) instead of imprisonment from 6 months to 2 years, plus fine.

Please note that, in this event, the penalty for fraud shall not complement the penalty for obtaining private electronic communications, confidential information or trade secrets by breaching computer devices, but will rather replace it.
Other Remedies

Selected Enforcement Actions/ General Comments

Although there is no specific law governing only data protection or privacy in Brazil so far, there are some data protection rules established in different pieces of legislation.

The recently enacted Internet Legal Framework is the Law which contains more specific provisions regarding data protection rules. This Law dedicates a chapter to the protection of logs, personal data and private communications made online. According to this Law, any collection, use, storage or processing of personal data requires the data subject’s express consent. Internet users shall give their express consent for the collection, use, storage, and processing of personal data, and such consent shall “stand out” from other contractual conditions, that is such consent should not be “hidden” amongst a website’s terms of use, where a “normal” user would not be able to easily identify it. Also, pursuant to the Internet Legal Framework, personal data may only be transferred to third parties upon the free, express and informed consent of the data subject and information stored by websites and the content of such private communications may only be disclosed upon a relevant court order.

Moreover, an individual’s right to intimacy, privacy, honor and image is considered a fundamental right subject to protection by the Brazilian Federal Constitution, and so any use of personal data, including the collection, processing, storage, disclosure and transfer thereof must be made in a way that the rights of intimacy, privacy, honor and image of the data subject are not infringed, under penalty of payment of indemnification for material or moral damages arising from such infringement.

Furthermore, the Brazilian Civil Code treats the right to privacy as a personality right, which cannot be waived or assigned as a matter of public policy.

Additionally, the Brazilian Consumer Defense Code (“CDC”) provides for certain rules regarding the storage and use of consumer data. In the absence of a specific privacy law, the principles and concepts of the CDC may apply by analogy to other types of relationships. In general terms, the CDC requires suppliers of products or services to previously inform the consumer about the storage of personal information in databases, if the consumer did not request such storage. The CDC also provides that consumers should have the right to access any information about them stored in databases and if any inaccurate information is stored in such files consumers also have the right to require the correction of such information. Moreover, the CDC prohibits the data controller from storing undesirable information about a consumer that refers to an event which occurred more than five years ago.

In view of the above, the conservative approach is to obtain the consent of Brazilian individuals prior to the collection, use, processing and transferring of any personal data whenever possible.
Canada

**Administrative Remedies**
The Canadian Privacy Commissioner has the power to investigate complaints, including compelling oral and written testimony and evidence. The Commissioner can also issue findings and recommendations; publish information about findings, and bring actions for non-compliance in Federal Court.

**Civil Remedies**
Individuals can file complaints with the Commissioner, and actions in Federal Court for actual and moral damages, and injunctive relief.

**Criminal Remedies**
Fines between $10,000 and $100,000 (Canadian Dollars).

**Other Remedies**
As of June 2015, Alberta is the only Canadian province to impose data breach notification requirements on organizations. However, commencing on an unspecified date in the future, all organizations in Canada except for those in the Canadian provinces of British Columbia and Québec will be subject to data breach notification requirements.

The Privacy Commissioner has the power to release the names of companies that breach privacy requirements if it feels that it is in the public’s best interest to do so.

**Selected Enforcement Actions/ General Comments**
In the 2013 case Chitrakar v Bell TV, [2013] FCJ No 1196, the Federal Court of Canada awarded an individual $10,000 in damages for breach of privacy, $10,000 in exemplary damages, and $1,000 in costs against a major telecommunications provider. In this case, the litigant was asked to sign a document upon receiving a TV box. The litigant testified that he believed he was signing only to confirm delivery, but his signature was affixed to a rental agreement that authorized the telecommunications provider to perform credit checks on him. The litigant later learned that the telecommunications provider accessed his credit history without his knowledge.

The court found that the telecommunications provider’s conduct constituted a breach of the litigant’s privacy rights and had adverse consequences. The court also awarded the litigant exemplary damages and costs due to the telecommunications provider’s conduct at the time of the breach of the privacy rights and thereafter. In particular, the court rebuked the telecommunications provider for failing to appear in the proceeding, subjecting the litigant to its ineffectual bureaucratic procedure, and generally disregarding the customer’s privacy rights.

In the 2012 case Biron v RBC Royal Bank, [2012] FCJ No 1183, the Federal Court awarded an individual $2,500 in damages for breach of privacy against a major Canadian bank. In this case, the litigant and her husband had a joint credit card account with the bank. At divorce proceedings between the litigant’s husband and the husband’s ex-wife, a representative of the bank disclosed credit card statements revealing the litigant’s personal information, despite her objections. The disclosures were not ordered by a court, and the litigant was neither a witness nor an interested party in the divorce proceedings. In assessing the quantum of damages, the court took into consideration the humiliation...
suffered by the litigant.

In 2012, certain Canadian provinces also began recognizing privacy-related torts, including intrusion upon seclusion, public disclosure of embarrassing private facts, publicity which places the plaintiff in a false light in the public eye, and appropriation of the plaintiff's name or likeness for the defendant's advantage (Jones v Tsige, 2012 ONCA 32). Private companies may be subject to liability for committing these torts. For example, in Evans v Bank of Nova Scotia, [2014] ONSC 7294, the Ontario Superior Court of Justice confirmed the certification of a class action against a major Canadian bank for, among other things, committing the tort of intrusion upon seclusion. In this case, an employee of the bank provided private and confidential information of bank customers to his girlfriend, who then disseminated the information to third parties for fraudulent purposes. The case is ongoing as of January 2015.

Efforts to comply with the findings and recommendations of the Privacy Commissioner can result in the expenditure of significant financial and human resources. In addition, the power to release names of specific companies can lead to negative publicity, as evidenced by recent focus on the privacy practices of social networking sites in Canada.
Colombia

**Administrative Remedies**

The Colombian Data Protection Authority, namely the Superintendence of Industry and Commerce ("SIC") has the power to investigate ex officio and based on complaints, alleged violations of data privacy and data protection rights of Colombian data subjects and of data subjects domiciled in Colombia.

The SIC can issue compelling orders to the managers of data bases to allow data subjects to access the data, to rectify and/or remove the data collected or processed in breach of the rights of data subjects; temporarily block the collected data as a precautionary measure; promote and implement educational campaigns on data protection rights, among others.

**Sanctions:**

The SIC can impose fines after the administrative investigation if it considers that the violation has been proven.

- Data controllers and processors can be subject to fines for breach of data protection regulations, which can be as high as 2.000 minimum legal monthly salaries (equivalent to COP 1.288.700 million during 2015 or approximately USD $545.000 at current exchange rates; these cap is updated annually).
- Successive fines could be imposed when the violation does not cease upon the order of the SIC.
- The SIC can order the temporary suspension of the activities related to the data processing, for a maximum period of six months;
- The SIC can order the permanent closure of the activities related with the data processing, if after the temporary suspension, the necessary corrective measures are not adopted;
- The SIC can also order the immediate and definitive closure of the activities related with the processing of sensitive data.

**Civil Remedies**

Data protection is a constitutional right, which is given a special and privileged protection by the Colombian Constitution. Individuals may bring a civil claim for monetary damages for any harm suffered for the violation of the constitutional rights to privacy and habeas data, and may also demand the suspension of the practice that gave rise to such violation.

**Criminal Remedies**

The Colombian Criminal Code establishes that acts or omissions that violate personal data protection rights, (including unauthorized collection, compilation, subtraction, offer, sale, exchange, interception, disclosure or modification of personal data), for ones benefit or that of a third party, will be subject to sanctions of imprisonment for a term between 48 to 96 months, and a fine of up to 1,000 minimum legal monthly salaries (equivalent to COP 644350 million or approximately USD $272914 at current rates; these cap is updated annually). The benefit that the criminal code provides for has been construed by local enforcement authorities to be a financial or economic one,
Other Remedies

Individuals may also bring constitutional actions ("acciones de tutela") before Colombian courts, when there is no other more expedited action to stop the violation of their rights or to prevent imminent damages.

Selected Enforcement Actions/ General Comments

Law 1581 includes references to the principle of accountability and a provision on Binding Corporate Rules, which will be subject to further regulation. It is anticipated that the BCR model will provide a more lenient treatment to companies and groups of entities that incorporate sound internal procedures for the adequate protection of privacy rights.

The SIC has started to take actions against managers of data bases who have breached data protection rights. Fines have been imposed for creating black client lists to deny services without complying with required procedures, collecting data in excess of the purpose of the collection, using data for cross selling without consent, among others.

Fines have been lenient so far and have not reached 10% of the maximum threshold. Because the regime is fairly new, the SIC has continued to apply a lenient trend in terms of amounts of fines, but this trend can change at any time and once all pending regulations are developed by the Colombian government. Some examples of recent enforcement action in Colombia include:

- In 2014 stem cells bank Red Cord was fined for COP 123 million (approximately USD $ 70,000) for the unconsented processing of sensitive personal data of women who tested positive for being pregnant in laboratory tests taken in a laboratory located in the city of Bogota.

- In 2014 the website www.datajuridica.com was temporarily foreclosed for the unconsented display of personal data. This site allowed to enter any Colombian ID number and made a false suggestion that the person under a specific ID, had a criminal court prosecution record.

- In 2012 the SIC imposed fines to mobile phone operator TIGO for collecting credit history data and consulting credit bureaus with respect to individuals that were buying pre-paid packages of mobile phone services. The SIC considered that the violation consisted of imposing on the individuals the obligation to provide redundant data that was not required for the purpose of the service (a pre-paid card did not trigger any credit risk for the service provider) and using it to consult the credit rating databases without consent from the data subject. Fines were of COP $11,334,000 (approximately USD $ 6,300).

- In 2011 telecom companies Telmex and UNE were subject to fines of COP 187 million each (approximately USD $ 100,000) for reporting individuals to credit bureaus for non-existent debts or obligations, or for reporting them for a period beyond the authorized term, after the fulfillment of their obligations with the telecom companies.
Mexico

Administrative Remedies

The Mexican Institute for Access to Information and Personal Data ("IFAI") has the power to initiate upon petition of interested parties or ex officio any action to verify compliance with the Mexican Federal Law for the Protection of Personal Data in Control of Private Persons (the "Data Protection Law") by data controllers.

The Data Protection Law provides data subjects with the right to enforce the protection of their Personal Data before the IFAI in cases where data controllers refuse to provide information about the Personal Data that it holds on the requesting data subject or refuse to rectify the Personal Data from errors, among others.

Upon notice of a resolution from the IFAI, data controllers have 10 days within which to comply with the resolution.

Civil Remedies

Data subjects may further seek indemnification from data controllers when they consider that they have suffered damages or losses derived from a breach by the data controller of the Data Protection Law.

Although there may be claims available for data subjects in connection with damages (including moral), these proceedings are not pursued due to the difficult procedure in evidencing the cause of the damages, the effect (directly caused by the action of the data collector or processor) and especially to quantify the damage.

Data subjects have the right to access, rectify the Personal Data from errors, cancel information kept by the data controller oppose the use for purposes other than those authorized to the data controller, and to revoke the authorization to process personal data.

Criminal Remedies

The Data Protection Law sets forth:

(a) Monetary penalties:

- Failure to comply with the Data Protection Law may result in monetary penalties that can reach approximately $1.5 million; and up to approximately $3 million when sensitive Personal Data is involved.
- Please note that according to the Data Protection Law, these penalties are exclusive of any claim for damages that could be filed by the data subject.

(b) Criminal liability:

- The Data Protection Law indicates that the act of compromising the security of a database containing Personal Data with the intention to profit is a criminal offence, which can be punished with up to 3 years of imprisonment; and up to 6 years when sensitive Personal Data is involved.

Furthermore, the act of collecting, using, disclosing or storing Personal Data through deceit of the data owners with the intention to profit is also considered a criminal offence punishable with up to 5 years of imprisonment; and up to 10 years when sensitive Personal Data is involved.
Other Remedies

Selected Enforcement Actions/ General Comments

Enforcement actions. IFAI has enforced fines in more than 20 cases between 2012 and 2013, for over 5 million USD total. IFAI has specially targeted the financial, telecom and health sector, but fines have been imposed in the services sector as well.

In a relevant case for the health sector, a Mexican Health and Addictions Treatment Institution was fined with more than $200,000 USD on charge of obstruction of justice. In the case, the clinical records of a data subject which was party to litigation in a case before the Supreme Court of Justice were provided to media, without data subjects consent. The leak caused a dramatic turn around in the public opinion with regard to case and the decision took by the Court. Clinical records were under the legal responsibility of the Institution, since the data subject has been treated there for mental disorders 25+ years before the data leak. IFAI followed an ex-officio investigation to find out the cause of the leak and whether the Institution had in place sufficient security measures to protect patient's information. The Institution prevented IFAI officers to examine security measures used by the Institution to protect personal data, which was viewed by the IFAI as obstruction of justice.

With regard to fines in connection to Banking and Telecom sectors, most of the fines imposed are related to cases of unsolicited emails, misuse of personal data for marketing purposes; in most cases, privacy notices were found to lack minimum mandatory information elements or were inconsistent with companies internal processes.

The Data Protection Law came into force on July 6, 2010, and is Mexico's first law at the federal level.

It creates a new set of obligations and compliance challenges for companies that collect, process, store or manage personal data in Mexico.

The Data Protection Law exempts the collection or storage of personal data strictly for personal purposes, without the intention to further divulge such information or use it for commercial purposes.

Certain Personal Data are regarded by the Data Protection Law as being sensitive personal data.

In general, the treatment of Sensible Personal Data requires additional attention and measures and its mishandling is subject to more stringent penalties.

In general, all data collectors must deliver a privacy notice to the data subjects (including employees) and appoint a person or group responsible for Personal Data-related requirements.
United States

**Administrative Remedies**

Gramm-Leach-Bliley Act ("GLBA"), Title V, 15 U.S.C. §§6801-6809 and its implementing regulations: The Federal Consumer Financial Protection Bureau ("CFPB") and the Federal Trade Commission ("FTC") as well as federal functional regulators and State insurance authorities have the power to enforce GLBA with respect to the entities within a particular agency's authority. The CFPB can initiate administrative adjudication enforcement actions against potential violators. The CFPB has established the Office of Administrative Adjudication, which is an independent judicial office within the CFPB. Penalties available in an administrative adjudication proceeding include those set forth in the next column, with the exception of civil monetary penalties.

The CFPB has the power to issue cease and desist orders, following notice to the alleged violator and a scheduled hearing.

FTC Act, Section 5 of the Federal Trade Commission Act, 15 USC § 45 ("FTC Act"): The Federal Trade Commission ("FTC") may bring an administrative hearing against an individual or entity suspected of unfair or deceptive trade practices in violation of the FTC Act. At the conclusion of such a hearing, the FTC may issue an order to cease and desist. The FTC If the individual or entity subject to the order violates that order, the FTC may issue administrative penalties of up to $16,000 per violation.

COPAA, the Children's Online Privacy Protection Rule, 16 CFR 312.1 et. seq., implementing the Children's Online Privacy Protection Act of 1998, 15 USC § 6501 et. seq. ("COPPA"): Violations of COPAA are deemed to be unfair or deceptive trade practices and are therefore subject to the same administrative penalties as set forth under the FTC Act, as described above. COPPA also gives states and certain other federal agencies authority to enforce compliance.

**Civil Remedies**

GLBA: The CFTC has the power to bring civil actions for damages. Penalties include: rescission or reformation of contracts; monetary refunds or return of real property; restitution; disgorgement or compensation for unjust enrichment; monetary penalties; public notification of the violation; limits on the violator's functions. Civil monetary penalties range from a maximum of $5,000 per day of violation to $1,000,000 per day of violation, where an individual knowingly violated the law.

FTC Act: The FTC may bring civil actions for civil monetary penalties of up to $16,000 per violation. Each day that non-compliance continues is considered a separate "violation" for purposes of the law.

COPAA: Violations of COPAA are deemed to be unfair or deceptive trade practices and are therefore subject to the same administrative penalties as set forth under the FTC Act, as described above. COPPA also gives states and certain other federal agencies authority to enforce compliance.

HIPAA, Standards for Privacy of Individually Identifiable Health Information, issued pursuant to sections 1171 through 1179 of the Social Security Act ("HIPAA"), as amended by the Health Information Technology for Economic and Clinical Health Act, Sec. 13001 of the American Recovery and Reinvestment Act, Public Law 111-005 ("HITECH Act"): The US
Department of Health and Human Services ("HHS") may impose a civil monetary penalty on any person who violates the HIPAA Privacy Standards, at an amount of between US $100 to 50,000 per violation, with a total of US $ 25,000 to 1.5 million for all violations of a single requirement in one calendar year.

**Criminal Remedies**

GLBA: While the CFPB has no power itself to bring criminal actions, pursuant to federal statute, if the CFPB obtains evidence that a person has engaged in conduct that may violate a federal criminal law, the CFPB is authorized to provide that evidence to the Attorney General of the United States, who will be able to investigate and potentially bring an enforcement action.

FTC Act: No criminal penalties specified.

COPPA: No criminal penalties specified.

HIPAA: Violations of the Privacy Standards include criminal penalties, including up to ten years imprisonment in certain cases. These penalties may be imposed on Business Associates as well as Covered Entities, as defined under the law.

**Other Remedies**

GLBA: The CFPB also has the power to undertake investigations of a potential violator by issuing a civil investigative demand. As part of its investigation, the CFPB can issue demands for production of documents as well as for giving oral testimony.

**Selected Enforcement Actions/ General Comments**

Federal Communications Commission: In October 2014, FCC fined TerraCome and YourTel American who "stored Social Security numbers, names, addresses, driver's licenses, and other sensitive information belonging to their customers on unprotected Internet servers that anyone in the world could access." The carriers will be fined $10 million for their breach of consumer privacy.

Federal Communications Communication: In September 2014, FCC reached a $7.4 million settlement with Verizon over privacy violations for its "use of personal consumer information for marketing purposes," according to a Federal Communications Commission press release. In addition, Verizon had to agree to a three-year compliance plan.

Health & Human Services: In May 2014, New York and Presbyterian Hospital (NYP) agreed to pay OCR $3,300,000 to settle potential violations of the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules by failing to secure thousands of patients’ electronic protected health information (ePHI) held on their network.
Venezuela

Administrative Remedies

There is no specific administrative entity in charge of privacy matters.

Most likely privacy cases will be decided in court and such entity will determine any applicable precautionary measures depending on the specific case.

Civil Remedies

The Law of Data Processing Crimes provides for civil sanctions that range from 200 tax units to 600 tax units. Currently, a tax unit is equivalent to Bs. 127 (which equals to USD 2.43 at the SICAD 2 official exchange rate of 52.10 per USD), subject to subsequent annual adjustments made by the Tax Administration normally within the first quarter of each year and according to the inflation of the preceding year.

Furthermore, in case of a civil judicial procedure, the court will determine the indemnification to be awarded to a plaintiff if damages are proven.

Criminal Remedies

Failure to comply with the provisions of the Law Protecting the Privacy of Communications, subjects the offender to sanctions of imprisonment that range from a minimum of three months up to a maximum of five years.

Failure to comply with provisions of the Law of Data Processing Crimes, results in imprisonment sanctions ranging from two years up to a maximum of six years.

Other Remedies

None.

Selected Enforcement Actions/ General Comments

The regulations contained in Venezuelan law in connection with data privacy and the transfer of personal data are limited to few provisions contained in (i) the Constitution of the Bolivarian Republic of Venezuela and, (ii) special laws which sanction certain conducts related with the violation of the right to data privacy.

As stated, it is very likely that any matter concerning privacy matters will be decided by a court.

Some examples of recent enforcement action in Venezuela:

- In a decision issued by the Supreme Court on March 14, 2001, the Court set forth an interpretation of Articles 28 (right to access official records) and 60 (right to the protection of privacy) of the Constitution. This leading decision (a) determined the privileged information that is protected under constitutional standards; and (b) established a habeas data process and the information that may be subject to such process (the “Decision”). In this respect, the Decision indicated that privileged information subject to constitutional protection is such information contained in one or more registries that combined could create a complete or partial profile of the individual whose data is included in such registry.
Based on the foregoing, under this decision it could be interpreted that an employer database complies with Constitutional standards, if from the information of the database one is not able to assert a complete profile of a registered person, i.e. an employee. It is important to indicate that the decision does not clearly define what should the expression “complete or partial profile” should mean.

Furthermore, on August 4, 2011, the Constitutional Chamber of the Supreme Tribunal issued Decision No. 1318 (“Decision 1318”), which is the first court decision that discusses the principles contained in Article 28 of the Venezuelan Constitution. Pursuant to Decision 1318, the main principles that regulate data privacy in Venezuela are the following:

- **The Autonomy of Will Principle** – Any person whose data are included in a database is entitled to be informed about: (i) the collection of his or her data; (ii) the entity responsible for her or her data; (iii) the purposes for which the data was gathered; and (iv) the manner in which he or she may exercise the right of self-determination. All these are subject to the existence of a “prior, free, informed, unequivocal and revocable consent” by the party affected, in the event the organization that is responsible for the data needs to disclose them.

- **Legality Principle** – The right to “information self-determination” can only be limited by means of rules having the rank of law, provided that this is justified by the public interest, and such rules must be interpreted restrictively. In this regard, the Chamber makes it clear that the information gathered (i) cannot be used for purposes that are contrary to the principles set forth in the decision under analysis or to constitutional guarantees; or (ii) processed by illegal or unfair methods.

- **Purpose and Quality Principle** – The organizations that wish to compile personal data of individuals must do so in strict compliance with the constitutional and sectorial laws and regulations, and this must be done with a clear purpose, reason or cause. This principle is deemed to be essential in order for the individual’s consent to be valid. According to this principle, the gathering and use of personal data of individuals must follow the principle of good faith and proportionality, for only the data that is adequate, pertinent and not excessive for the purpose sought can be gathered.

- **Temporality and Preservation Principle** – Based on the right to protection of data, intimacy and to update the information contained in databases and in files of public and private persons, the Chamber held that the information contained in such systems must be updated regularly in order to avoid impairment to individuals as a result of obsolete data. In addition, the Chamber adopted the decisions adopted by Colombian courts regarding the “right to oblivion,” which is the right of all individuals to have their personal data updated once a default or tardiness incurred has been remedied.

- **Accuracy and Self-Determination Principle** – The personal data must reflect the true condition of the individual. In this regard, the data must not only be up-to-date, but accurate and complete as well. In order to achieve the efficacy of this principle, clear and expedite procedures must be set-up in order to ensure that the individuals have access to and knowledge about the data kept by public and private institutions about them. This also implies the right of individuals to demand the rectification or cancellation of incomplete, inaccurate, inadequate and excessive data, and
to be advised of their correction.

✓ Foresight and Integrality Principle – Technological advances require an analysis of the storage, compilation and use of personalized data jointly with other databases or records in which the individual’s personal data is stored, since if shown as a whole, they may be prejudicial to the individual or his or her interests or rights.

✓ Safety and Confidentiality Principle – All entities that handle the compilation, storage and use of databases have the obligation to keep the required security regarding such data, and to prevent the modification thereof by unrelated third parties. This obligation remains even after the termination of the relationship between the entity and the relevant person. Additionally, the Chamber stated that this principle includes the prohibition to transfer the contents of databases to other states that do not have rules that guarantee the protection of the individuals’ information.

✓ Protection Principle – Judicial protection is not sufficient. It is necessary to have public entities with jurisdiction to prepare and implement models based on technical standards whereby the information in these databases is protected.

✓ Responsibility Principle – Any infringement of the right to protection of data will give rise to civil, administrative and criminal penalties. The liability for the breach of this right will not only fall on the officer in the banking sector, but also extends to any other sector in charge of information system.
## Austria

### Administrative Remedies

The Austrian Data Protection Authority (DPA) has the power to investigate complaints and cases, and to order the suspension of processing and/or transfer of data, as well as destruction of data; these orders can be appealed to the Federal Administrative Court.

Administrative penalties for infringement of Austrian Data Protection Act amount to fines of up to €10,000 (for negligent violations) or up to €25,000 (for willful violations).

### Civil Remedies

Individuals can file complaints with the DPA, and can seek a judicial remedy, including an injunction, for violations of the law. In case of employee data protection violations, the works councils, if one exists, can obtain a preliminary injunction from the Employment Court.

Furthermore, damages can be sought according to general civil law.

### Criminal Remedies

The Austrian Data Protection Act provides a criminal sanction of up to 1 year imprisonment in case of intentional misuse or intentional unauthorized transfer of such data to third parties.

In addition, the Austrian Criminal Code envisages criminal sanctions for illegal access to computer systems (hacking), abusive interception of data, data damaging (illegally changing, deleting or making data unusable), misuse of computer programs or fraudulent misuse of data processing.

### Other Remedies

Infringement of the provisions of the Austrian Data Protection Act may allow consumer protection organizations as well as competitors to obtain an injunction under the Austrian Act against Unfair Competition.

Furthermore, press coverage of infringements of data protection law may lead to serious damage to reputation.

### Selected Enforcement Actions/ General Comments

Administrative sanctions are not imposed by the DPA but by local authorities. In the city of Vienna, there are approx. 40 proceedings per year in which sanctions are imposed.

As regards criminal sanctions, there has, so far, only been a single case that was publicly reported.

Private enforcement has recently received significantly more attention. In July 2014, Max Schrems filed a quasi-class action a social media company in the Commercial Court Vienna. More than 25,000 users of the social media platform from all around the world had assigned him their rights to claim damages from the social media company for various alleged privacy violations. Currently, the Commercial Court Vienna is still considering social media company's arguments against Austria's international jurisdiction. This case illustrates that private enforcement can be a very significant risk for high-profile corporations.
Belgium

**Administrative Remedies**
The Belgian Privacy Commission (Belgian Data Protection Authority) has no power to impose administrative fines, sanctions or measures in case of violations of the Data Protection Act yet (it being noted that a legislative change is expected in the near future to allow the Privacy Commission to impose sanctions). It has, however, the power to investigate cases (including requesting documents and making on-the-spot investigations), handle complaints and carry out mediation procedures, issue non-binding advice, and submit civil cases to the Court of First Instance and criminal cases to the public prosecutor.

**Civil Remedies**
Individuals can file claims with the President of the Court of First Instance to obtain injunctive relief (e.g. suspension of processing) and actual damages.

A data controller is liable for any damage caused by an act in violation of the Data Protection Act, unless it can prove that it did not cause the damage.

An individual may also file criminal claims.

**Criminal Remedies**
Fines of between €600 and €600,000 and/or same fines and imprisonment from 3 months to 2 years (in case of second offences) depending on the violation.

In addition, Belgian courts may, as the case may arise, order publication of their decisions in whole or by excerpt in one or more newspapers, as well as the seizure of any privacy infringing equipment or data, and rectification or destruction of personal data; courts may also prohibit the controller from processing any personal data for up to 2 years.

Legal entities may face criminal sanctions up to, and including, their forced winding up.

**Other Remedies**
Under Belgian law, both legal entities and individuals can be prosecuted for criminal offenses.

Company officials and other employees can potentially be held criminally liable for acts of the company if they have personally participated in the act or omission that violated the law.

In practice, non-compliance with the Data Protection Act creates concerns for an employer because it may be difficult or even impossible (although case law is evolving in that respect) to make use of the data gathered in violation of the Data Protection Act to dismiss and/or prosecute an employee.

Certain labor courts, notably in the frame of cases of alleged abusive dismissal of employees, have granted indemnities to employees whose privacy rights had been infringed by their employer (see notably the Labor Court of Gand, Decision of October 14, 2011, where the Court granted an indemnity evaluated *ex aequo et bono* at €1).
Some examples of recent enforcement action in Belgium include:

In 2007, the Belgian Privacy Commission and the Article 29 Working Party opened an investigation against SWIFT, a Belgian-based financial payment provider, with respect to data transfer and sharing activities with the US government. SWIFT was subjected to 2 years of investigations, and eventually settled the dispute by agreeing to join the US-EU Safe Harbor Privacy Agreement, establishing new information technology infrastructure for European transactions in Switzerland, and taking other steps. In November 2013, the Belgian Privacy Commission launched a new investigation, together with the Dutch Data Protection Authority, on the security measures implemented by SWIFT. In May 2014, the Belgian and Dutch data protection authorities indicated that they had not recorded any violation of legal security requirements by SWIFT.

Over the last three years, the Belgian Privacy Commission appears to have taken a more aggressive stand vis-à-vis potential privacy violations and seeks to impose out-of-court pecuniary settlement on alleged infringers through the public prosecutor’s office.

For instance, in January 2011, the federal public prosecutor’s office opened an investigation at the suggestion of the Belgian Privacy Commission regarding personal data transmitted by wireless devices that were arguably illegally intercepted. In August 2011, the firm concerned received an offer for an out-of-court settlement subject to the payment of €150,000 from the Belgian federal prosecutor.

In a recommendation of January 2013 on information security, the Privacy Commission indicated that, in case of non-compliance with its recommendations in that respect, it would make its best efforts and use all legal means to have data controllers held liable, including through criminal prosecution by referring the case to the public prosecutor. In April 2013, for the first time, the Belgian Privacy Commission announced that it referred a security breach case to the Brussels Public Prosecutor to initiate criminal proceedings. This case concerned the National Belgian Railway Company.

At the end of 2014, the chairman of the Belgian Privacy Commission told the press that one of the biggest cases they had been working on involved a pharmaceutical company. He also announced the creation of a new investigation department within the Privacy Commission, that will actively investigate violations of the data protection legislation and will focus on controllers processing sensitive data such as insurers and hospitals; this could thus also concern pharmaceutical and/or cosmetic companies handling health-related data.

In June 2015, after a recommendation issued in May, the Belgian Privacy Commission initiated legal action before the Court of First Instance against a social network company. The case is pending and should be pleaded in September 2015.

It is worth noting that not being privacy/data protection compliant generally may result in having to deal with the Belgian Privacy Commission, which is particularly relentless in the pursuit of its demands.

Bad press coverage is generally the most common sanction that companies will face in Belgium.

Criminal sanctions are rare and have been so far reserved to material violations or reckless ignorance of the data protection law.
Czech Republic

Administrative Remedies

The Czech Data Protection Office (“the Office”) has the power to investigate complaints and cases, and to impose penalties for breaches of the data protection act; penalties can be up to CZK 10,000,000 (approx. 500,000 USD) and penalties can be imposed repeatedly if the same breach is also committed repeatedly.

Liability for a particular offence ceases to exist if the Office fails to commence administrative proceedings within a year from the date on which the Office learned about the breach, however no later than three years from the date of the breach.

Civil Remedies

Individuals can seek judicial remedies and damages for breach of the protection of their personhood.

Criminal Remedies

An individual found guilty of the unauthorized disposal of personal data may be punished by imprisonment for a term of up to 8 years. Legal entities may not be criminally liable for unauthorized disposal of personal data.

Other Remedies

None.

Selected Enforcement Actions/ General Comments

Some examples of recent enforcement action in the Czech Republic include:

✓ A fine of CZK 3,500,000 was imposed by the Data Protection Office on Komerční pojišťovna, a.s. for the leakage of client data.

✓ A fine of CZK 100,000 was imposed on Eurotel for misplacement of documents containing personal data.

✓ A fine of CZK 2.3mil was imposed by the Data Protection Office on the State Institute for Drug Control for the unauthorized processing of health data of patients.

✓ A fine of CZK 160,000 fine was imposed on Scarabeus, a B2B company for the breach of rules for sending commercial messages via email (anti-spam rules).

✓ A fine of CZK 300,000 was imposed on GE Money for the unauthorized processing of telephone contacts to potential clients of GE Money Bank, GE Money Auto and GE Money Multiservis.

✓ Many companies investigated for operation of cameras at the work site and thus encroaching employees’ right to protection of privacy.

✓ A fine of CZK 450,000 was imposed on the Ministry of Education by the Data Protection Office for the leakage of personal data of pupils attending schools which were awarded grants by the Ministry of Education.

✓ A fine of CZK 100,000 was imposed on the Chief public prosecutor by the Data Protection Office for the publication of
wages of employees of the Chief public prosecutor’s office.

- A fine of CZK 1,8mil was imposed by the Data Protection Office on Komerční banka for the leakage of clients data.
- A fine of CZK 450,000 was imposed by the Data Protection Office on the Ministry of Education for the online publishing of personal data of pupils who received grants to study.
Denmark

**Administrative Remedies**

The Danish Data Protection Agency has the power to investigate complaints and cases, and to order the suspension of processing and/or transfer of data, as well as the destruction of data and other similar actions; these orders can be appealed to the courts.

**Civil Remedies**

Individuals can file complaints with the Agency and can seek a judicial remedy for violations of the law, for example damages pursuant to the general civil law.

**Criminal Remedies**

The Danish Act on Processing of Personal Data states two types of criminal sanctions - fines and imprisonment for up to 4 months. Only natural persons are subject to imprisonment and generally, imprisonment as a sanction is less likely.

Further, the Danish Criminal Code envisages criminal sanctions for hacking, e.g. illegal access to IT systems, user profiles on social media, e-mail accounts and other programs that is a property of others. The criminal sanctions are fines and imprisonment for up to 1 year and 6 months (however, up to 6 years under aggravating circumstances).

**Other Remedies**

Any employee who has intentionally or negligently infringed the Danish Act on Processing of Personal Data may be subject to punishment.

The Danish Data Protection Agency has authority to publish its decisions on the website (www.datatilsynet.dk) which may lead to unwanted publicity and damage to reputation.

**Selected Enforcement Actions/ General Comments**

It is uncommon to issue fines as means of sanctioning and the Danish Data Protection Agency usually would give a reprimand and state a deadline for achieving compliance with the requirements. If these initiatives are ignored, the legal entity in question might be reported to the police and thus fined.

The highest fine to date was imposed in 2001 and was set at DKK 25,000 approx. €3,360. However, in the light of international practice the fine level in Denmark is expected to increase.
Finland

**Administrative Remedies**
The Finnish Data Protection Authority (the Office of the Data Protection Ombudsman) has the power to investigate complaints and cases (including requesting documents and making on-the-spot investigations); issue non-binding advice; submit matters to the Data Protection Board for prohibition; submit criminal cases to the public prosecutor, and to order the suspension of processing and/or transfer of data, as well as the destruction of data and other similar actions; these orders can be appealed to the courts.

**Civil Remedies**
Individuals can file complaints with the authority, and can seek a judicial remedy for violations of the law.

**Criminal Remedies**
Serious breaches are classified as “personal data file crimes”, and are punishable by up to 1 year imprisonment.
Less serious breaches are classified as “personal data violations” and are punishable only by fines.

**Other Remedies**
Directors, officers or employees may be liable to compensate their employer for damages that the employer incurs and may also be subject to criminal charges.

**Selected Enforcement Actions/ General Comments**
There is limited case law in Finland related to breach of the data privacy regulation.

In its case 1998:85, the Supreme Court regarded a disclosure (sale) of a personal data file to another company for a different purpose of use as an infringement of the privacy of data subjects and found the representatives of the company guilty of infringing the law (criminal liability). According to the Supreme Court, infringing the privacy of a data subject in itself constitutes damage or injury.

As the Finnish Data Protection Authority has no authority to impose fines, the Finnish enforcement is mainly based on correcting violations by giving guidance and advice to the data controller.
France

Administrative Remedies
The Data Protection Authority ("CNIL") has the power to investigate (on-site or on-line) complaints made by individuals and to investigate any company based on the CNIL’s annual investigation program, any complaint by an individual, or any public information (e.g. press release concerning a data breach).

The CNIL may decide to: order that the company complies with French data privacy law and/or files the appropriate formalities; order the suspension of any processing and/or transfer of data, as well as the destruction of data and other similar actions. Any decision of the CNIL may be appealed to the courts.

Breaches of data privacy laws are as follows:

- Regulator/administrative fine from the CNIL: €150,000 and €300,000 in case of relapse.

Civil Remedies
Potentially limitless. This concerns any civil action brought as a result of damages due to a breach of French privacy law by the controller and/or processor.

Criminal Remedies
Criminal sanctions of up to €300,000 for an individual and €1,500,000 for an entity; and up to 5 years imprisonment; the sentence is published in the national press.

Other Remedies
There are also reputational consequences to consider, because the CNIL has the authority to advertise any decision or sanction taken against a company.

Selected Enforcement Actions/ General Comments
Some examples of recent enforcement action in France include:

- On December 11, 2007, Service Innovation Groupe France (SIG) was fined €40,000 for inappropriate comments contained in the employee management file.

- On April 16, 2006, Jean Marc Philippe company was fined €10,000 for installing a CCTV system that permanently monitored its employees. In addition, the General Manager was fined €5,000 by a criminal court for objecting to the CNIL’s investigation.

- On June 28, 2006, Crédit Lyonnais was fined €45,000 for failing to respond to the CNIL’s requests regarding the abusive registration of multiple clients in a central file of persons that had payment difficulties (FICP) that is managed by the Banque de France.

- On November 23, 2006, Crédit Agricole France (Bank) was fined €20,000 for having processed personal data within the National Register on Household Credit Repayment Incidents (FICP) with no valid justification and insufficient
guarantees in respect of technical and organizational security measures.

✓ On December 14, 2006, Tyco Healthcare France was fined €30,000 for having improperly transferred its employees’ personal data to its headquarters in the US and failing to answer the CNIL’s requests on the purposes of the processing, location of servers and systems, recipients of the data and safety measures applied to such data.

✓ On April 22, 2010, the CNIL sanctioned Acadomia company with a public warning for the collection of excessive comments regarding their clients, unlimited data retention periods and non-compliance with prior data processing formal requirements. Several newspapers published articles in May 2010 after CNIL’s investigation e.g. in Figaro: “Scandal surrounding Acadomia’s files,” in Le Monde “CNIL severely collar Acadomia,” Les Echos “the bad behavior of Acadomia.”

✓ On March 17, 2011, an internet search engine company was fined €100,000 for committing the following breaches:
  ✓ Absence of notification of latitude application despite the notice sent by the CNIL;
  ✓ Absence of proper information on the processing of Wi-Fi data collected by the internet search engine company car;
  ✓ Incomplete information on the source code of the software capturing the payload data.

✓ On February 26, 2009, Directannonces, a company specialised in compiling real-estate offers from individuals found on the Internet and selling these information to real-estate professionals, was fined €40,000 because such practice was considered as an unfair collection of personal data, and Directannonces had not collected the data subjects’ prior consent resulting in the impossibility to object to such processing.

✓ On January 12, 2012, GROUPE DSE France was fined €20,000 for having solicited individuals by telephone who did not consent to telephonic prospecting. GROUPE DSE France had purchased their contacts from partnering vendors.

✓ On June 22, 2012, Equipement Nord-Picardie was fined €15,000 for failing to ensure for one of its employees the right of access to his personal data and failing to answer the CNIL’s requests on the procedure set up to handle employees access requests to their personal data.

✓ On May 30, 2013, PS CONSULTING was fined €10,000 for having implemented a CCTV system that permanently monitored its employees with no valid justification by regards to the purposes for which these data are collected or are further processed. In addition, the employees were not informed of such a monitoring framework. Finally, PS CONSULTING was not able to provide an adequate security to the personal data it had collected.

✓ On October 24, 2013, AOCT was fined €10,000 for having not carried out the formalities that must be satisfied before the implementation of a CCTV system. Furthermore, the employees were not informed of the existence of such a system. Moreover, the CNIL noticed an absence of responses despite the requests sent by the CNIL.

✓ On 3 January 2014, the CNIL’s Sanctions Committee issued a 150 000 € monetary penalty to an internet search engine company upon considering that the privacy policy implemented since 1 March 2012 does not comply with the French Data Protection Act.
On January 29, 2014, the association JURICOM & ASSOCIES was fined €10,000 for not having guaranteed the right of its members to object to the processing of their personal data.

On August 7, 2014, the CNIL sanctioned Orange with a public warning. The company didn’t audit its service provider’s security measures before using their services. Besides Orange transferred its client’s personal data to the service provider without any security or confidentiality clauses having been decided.

On June 6, 2015, Prisma Media was fined €15,000 for having prospecting individuals by mail. Consent was given for the receiving of an informational newsletter but not explicitly for prospection.
Germany

**Administrative Remedies**
Different data protection authorities in each Federal State have the power to investigate complaints and cases, and to order the suspension of processing and/or transfer of data, as well as the destruction of data and other similar actions; these orders can be appealed to the courts.

**Civil Remedies**
Individuals can file complaints with data state protection authorities, and can seek a judicial remedy for violations of the law.

Warning letters by data subjects, asking the violating party to sign a cease-and-desist declaration. The violating party has to refund the costs for such letters, including attorney’s fees, which may well add up to approximately €1,500 in each individual case. Where the violating party is an enterprise, warning letters may also be sent by competitors, consumer protection organizations and special interest organizations.

Consumer protection bodies may issue cease-and-desist letters and also start court proceedings where data protection provisions are to be part of general terms and conditions from a consumer’s point of view. In the future these rights are likely to be extended; they may then cover any breach of data protection provisions.

Claims for injunctive relief in case the violating party does not sign a cease-and-desist declaration. The violating party may also have to refund the additional costs, which would probably range at around €2,500 in each individual case.

Compensation claims for damages suffered by data subjects and/or competitors and related claims regarding the disclosure of information required to calculate such damages. In most cases, however, it would already be difficult to prove the existence of damages.

Claims for profit: If the same type of violation was committed intentionally in a number of cases, the violating party’s profits may be skimmed off and deferred to the state budget. However, this sanction is rarely applied in practice.

**Criminal Remedies**
Fines of generally up to €300,000 (may be exceeded if the infringement led to higher profits) and up to 2 years imprisonment

**Other Remedies**
Works councils can file for preliminary injunctions against employers preventing them from putting into operation data processing systems.

An employee, manager, director or other individual might also incur liability in tort.
Some examples of recent enforcement action in Germany include:

- In 2008, Deutsche Telekom was fined €1.4 million for illegally checking on connection data of phone calls of managers, board members, and others suspected of leaking company confidential information.

- In 2010, Lidl AG, a grocery chain that had allegedly illegally spied on employees with cameras during work hours and that had failed to appoint a DPO, was fined with an overall amount of €1.46 million.

- In a similar case of illegal CCTV surveillance of employees, in 2008 a fine of only €80,000 was levied on Tönnies, one of Europe's largest butcheries.

- In October 2009, Deutsche Bahn AG accepted a fine in the amount of €1.1 million for screening employee data and comparing it to supplier data in an effort to combat corruption, but without specific suspicions related to individual employees. Also, the CEO was forced to step down, amongst other things for poorly handling this data protection incident.

- In May 2010, the Data Protection Authority of the German state of North Rhine-Westphalia levied a fine of €120,000 on Deutsche Postbank AG for allegedly having granted read access to customer accounts to self-employed agents for sales purposes, who thus gained visibility regarding the then-current financial situation of the customers.

- In a similar case, in November 2010, the Data Protection Authority of Hamburg levied a fine of €200,000 on Hamburger Sparkasse (Haspa) for allegedly having granted read access to customer accounts to self-employed agents for sales purposes, who thus gained permanent visibility regarding the then-current financial situation of the customers.

- In 2011, the financial-services provider “Easycash” was fined €60,000 by the North Rhine-Westphalian Data Protection Authority for transferring customer data regarding debit cards to a subsidiary and eventually to a third party that statistically analyzed these data.

- In June 2013 a fine (amount not made public) was levied upon a trade enterprise by the Bavarian Data Protection Authority for disclosing a large number of e-mail addresses to each of the recipients of the respective e-mail by sending the email via “Cc” instead of “Bcc”.

- In 2013 and 2014, Frankfurt and Berlin courts decided that certain terms and conditions (including data protection provisions) of certain tech companies were invalid and issued injunctions accordingly.

- In its activity report for 2013/2014, the Bavarian Data Protection Authority states that it has imposed administrative fines in the amount of total €200,000 in 117 fine proceedings in 2013 and 2014. According to their report for 2014, the Data Protection authority of the German state of Berlin levied administrative fines in the amount of total €88,205. Note that this is only one out of 16 data protection authorities in Germany.

- In 2014, the Data Protection Authority of the German state of North Rhine-Westphalia imposed a fine of €64,000 on a petrol station operator with nationwide subsidiaries due to unlawful video-monitoring of customers and employees. In 2014, a German relief organization for mentally ill people was fined €18,000 by the Data Protection Authority of the
German state of Schleswig-Holstein because of insufficient access protection concerning sensitive patient data.

☑ In December 2014, the regional German data protection authority (DPA) of Rhineland-Palatinate imposed a record fine of EUR 1.3 million on an insurance company. The sales staff allegedly sought address data of administration customers’ employees in order to offer them insurance products. Also, the public prosecutor initiated investigations against five employees because of an alleged incitement of civil servants to violate secrecy obligations and data protection laws by disclosing details on other officials in order for the insurance company to market services to them. The German Federal Financial Supervisory Authority (BaFin) conducted an investigation and required various improvements of the company’s data protection organisation.
Greece

Administrative Remedies
The Data Protection Authority has the power to investigate complaints and cases; issue warnings with orders to cease any violation within a specific time limit; issue administrative fines ranging between €880.41 and €146,735.14; temporarily and definitively revoke permits (only for serious or repeated breaches); and order the destruction of files or a ban of the processing and the destruction, return or locking of the relevant personal data (only for serious or repeated breaches).

Fines may be imposed in conjunction with an order for the revocation of permits and the destruction of files.

The Data Protection Authority also has the power, among others, to proceed ex officio or following a complaint, to conduct administrative reviews regarding the infrastructure supporting the processing of data.

It has the power to examine complaints of data subjects relating to the implementation of the Law on the Protection of Individuals with regard to the Processing of Personal Data (PIPPD); impose administrative sanctions and denounce any breach of the provisions of PIPPD to the competent administrative and judicial authorities.

The DPA can also refer the case to the competent Public Prosecutor, in case criminal charges are involved.

Civil Remedies
Individuals can bring claims for compensation and material damages caused in breach of the PIPPD before the civil courts.

The compensation amount payable for non-pecuniary damages caused in breach of the PIPPD is set at a minimum of €5,869.40, unless the data subject claims a lesser amount or the said breach was due to negligence.

Criminal Remedies
Fines range between €2,934 and €29,347 depending on the violation and up to 5 years imprisonment (or sometimes more under certain circumstances).

DPA officers are deemed as special investigating officers having all the powers invested in them by the Code of Criminal Procedure. They are entitled to carry out a preliminary investigation, even without an order from the Public Prosecutor, in case of acts which are caught in flagrante delicto, a misdemeanor, or if there is a risk of any delay.

Other Remedies
Data subjects are entitled to object at any time to the processing of data relating to them. Such objections could contain correction, temporary non-use, locking, non-transfer or deletion.

Selected Enforcement Actions/ General Comments
Some examples of recent enforcement action since 2012 in Greece include:

- €50,000 fine imposed on a financial institution due to a failure to safely destruct data files and violating the right to access of their data to data subjects;
• €30,000 fine imposed on a private company for violating the right to object to data subjects;
• €30,000 fine imposed on a financial institution for violating the obligation for lawful process of data (processing of non-accurate and not updated data) and the right to object to data subjects;
• €30,000 fine imposed on a company providing telecommunication services for violating the right to object to data subjects and unlawful interconnection of files;
• €15,000 fine imposed on a private company for violating the right of access of their data to data subjects;
• €10,000 fine imposed for unlawful publication of sensitive data;
• €4,000 fine imposed for violating the right to information of a data subject and
• Greek Civil Courts decisions adjudicated to data subjects amounts from €3,000 up to €15,000 for moral damages caused by the violation of the PIPPD.
Hungary

Administrative Remedies

The Hungarian National Authority for Data Protection and Freedom of Information ("Authority") has the power to investigate cases upon receipt of a complaint or *ex officio*. If the Authority commences a formal supervision procedure, the Authority may establish infringement of the Data Protection Act; prohibit illegal data processing; order the blocking or deletion of data; order the suspension of data processing; and prohibit data transfer abroad. The Authority may order the publication of the name of the data controller if the decision applies to a large number of data subjects and if publicizing the decision serves the interest of data protection. The Authority also is authorized to impose a data protection fine on a data controller if the Authority determines that material provisions of the Data Protection Act were infringed. The fines may range from HUF 100,000 (approx. €333) to HUF 10 million (approx. €33,333) in the Authority's discretion, depending on the facts and circumstances of the case. However, with effect from October 1, 2015, the Authority will be authorized to impose a fine of up to HUF 20,000,000 (approx. €66,666).

The Authority's decisions may be challenged before a court.

Civil Remedies

A data subject who believes that his/her rights have been infringed may institute court proceedings against the data controller. The data controller is liable for any damage to personal rights suffered by a data subject as a result of the unlawful processing of personal data or the infringement of the technical requirements of data protection. In case of such harm, the data subject may request a court: to establish the infringement of his/her personal rights; to require the cessation of the infringement or the granting of satisfaction (i.e., ordering, at the expense of the infringer, the prominent displaying of the operative part of the court's decision or any other corrective statement requested by the applicant); to hand over to the data subject the financial gains achieved through the infringement; and compensation for damages. The data subject also may claim exemplary damages (lump sum damages) which a court may award to compensate for the harm to personal rights (such as data protection rights) which occurred due to the data controller's unlawful data processing or breach of data security requirements. In the claim for exemplary damages, the data subject is not required to evidence the existence of harm beyond the mere breach of data protection laws.

Criminal Remedies

The Penal Code (Act C of 2012) penalizes the breach of the provisions of the Data Protection Act, including data processing for unjustified or unauthorized legal purposes, the violation of the requirement to provide notice or any omission of data security requirements – if the breach is committed for financial gain or if such illegal conduct causes significant detriment to the data subject or to others – with up to one year's imprisonment. A higher penalty (of up to two years' imprisonment) applies if sensitive data (i.e. personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, health data or sex life) was the subject of the criminal conduct.

Other Remedies

An executive officer of a legal person and the individual responsible for data processing each may be held liable for the legal person's non-compliance with data protection requirements if such non-compliance constitutes a crime.
Under the Act on the Measures Applicable to Legal Entities under the Criminal Code (Act CIV of 2001), if a shareholder, officer or an employee of a legal entity committed a crime aimed at or resulting in the legal entity gaining financial advantage and such conduct could have been prevented by the executive officer by fulfilling his supervisory or control duties, a criminal court may impose a fine equal to at least 500,000 HUF (approx. €2,500) and at most three (3) times the amount of the financial advantage gained or intended to be gained by the legal entity through the criminal act. If the amount of the advantage cannot be estimated or is difficult to estimate, the criminal court may make its own estimate and assess fines accordingly.

The Authority has been operating since January 1, 2012. In 2012, the Authority conducted 33 administrative procedures and as a result, issued fines in a total value of HUF 33 million (approx. €106,000). In 2013, the Authority conducted 41 administrative procedures and issued fines in a total value of HUF 49 million (approx. €160,000). In 2014, 30 administrative procedures were conducted and the total amount of data protection fines imposed by the Authority was HUF 45 million (approx. €150,000).

The Authority tends to impose fines only in cases in which it determines that a serious infringement of the Data Protection Act occurred. Other non-monetary sanctions are used more frequently by the Authority than monetary sanctions.

In 2013, the Authority’s examinations focused on the following areas: data processing activities relative to websites, in particular the processing of minors’ personal data in the course of their registration to website; and data processing in regard to debt management and recovery. In 2014, the Authority focused on product presentation events and continued to focus on data processing relative to debt recovery. In 2015, the enforcement priorities of the Authority are investigations relating to the data processing activities of debt collection agencies, data processing for product presentation events (“roadshows”), as well as data processing for telemarketing purposes.

The Authority has imposed the maximum fine on data controllers several times, including in the following cases:

- in August 2012, the Authority fined a Slovak entity Weltimmo s.r.o., an online real estate agent, for its failure to comply with statutory requirements under the Data Protection Act, including failure to provide notice and obtain consent, lack of a purpose limitation to the data processing, the processing and transfer of data without a valid legal basis and not complying with data subjects’ access and deletion requests. This case is currently pending before the Kúria (the Supreme Court of Hungary) and has been submitted to the CJEU for a preliminary ruling under case Nr C-230/14.

- in 2014, the Authority issued several decisions imposing penalties on companies conducting product presentation roadshows, which were found to have illegally collected health data from vulnerable consumers; including in September 2014 on a roadshow company conducting illegal data processing operations and again in April 2015 on a roadshow company for illegally processing personal data and sensitive data of consumers and for not complying with data subjects’ access and deletion requests;

- in December 2014, the Authority issued the maximum fine on a telemarketing company for failing to comply with
consent, notice, registration and data security obligations; in March 2015, the Authority fined another telemarketing company creating direct marketing databases without properly informing data subject that their data may be sold to third parties and for not keeping accurate active filings in the data protection register.

As there are very few published court cases addressing the breach of the Data Protection Act, no general conclusions can be drawn about the courts’ approach to the imposition of civil and criminal remedies. Moreover, such court decisions are based on the particular facts and circumstances of each case, and Hungarian courts are not required to follow the decisions of higher or equally ranked courts (other than Kúria decisions adopted in the interest of uniform legal interpretation and Constitutional Court decisions).

The Authority’s decision may be appealed at court based on a material legal issue (such as the alleged wrongful interpretation of the law) or on procedural grounds. If, on appeal, the court, finds that the Authority breached the applicable administrative procedural rules or misinterpreted a provision of applicable law, then the court must require the Authority to conduct new proceedings, as the courts do not have the authority to overrule the Authority’s findings on appeal.
Ireland

Administrative Remedies

The Data Protection Commissioner ("DPC") has the power to:

1. Investigate complaints and cases. It is under a mandatory obligation to investigate when complaints are received from individuals. It can also carry out investigations of its own accord where it believes there may have been a breach of the Data Protection Acts 1988 and 2003 ("DP Acts");

2. Appoint an authorized officer who has the power to enter premises of a data controller or data processor and to inspect the type of personal information kept, how it is processed and the security measures in place;

3. Compel data controllers to comply with the Data Protection Acts by issuing an enforcement notice to;

4. Obtain information from anyone by way of an information notice in order to pursue an investigation;

5. Order the suspension of processing;

6. Issue a prohibition notice to a data controller or data processor in order to prohibit the transfer of data from Ireland to a place outside Ireland; and/or

7. Order the destruction of data and other similar actions.

These orders can be appealed to the Circuit Courts within 21 days.

Civil Remedies

Individuals can file complaints with the DPC. The DPC will then be required to carry out investigations and may issue an enforcement notice.

Individuals can also sue for breach of duty of care in the courts provided they can prove that the breach was caused by failure of the data controller.

Criminal Remedies

Fines of up to €3,000 for summary conviction and up to €100,000 for conviction on indictment are applicable to offences under the DP Acts.

A data controller found guilty of an offence under the DP Acts can be fined the amounts listed above and/or may be ordered to forfeit or destroy or erase any data which the court may determine to be connected with the commission of the offence.

Summary proceedings for an offence under EC (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011 (S.I.336 of 2011), may be brought and prosecuted by the DPC. Each call or message can attract a fine of up to €5,000 on summary conviction. If convicted on indictment, the fines range from €50,000 for a natural person to €250,000 for an entity.

The court may also order the destruction of data that is connected with the commission of an offence.
**Other Remedies**

A director, manager, secretary or other officer of a corporate body, including employees in some circumstances, may be held liable for an offence under the DP Acts where such offences were committed with their consent.

**Selected Enforcement Actions/ General Comments**

The DPC publishes an annual report naming, in certain cases, those data controllers that were the subject of investigation or action by the DPC during the previous year.

1. **Breach of the EC (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011 (the "2011 Regs")**

   The ODPC successfully prosecuted a number of companies in the Irish courts for unsolicited direct marketing offences in breach of the 2011 Regs in 2013. Typically companies are prosecuted after "two strikes" ie where they have failed to heed a prior formal warning by the ODPC, however that is not to say that the ODPC would not prosecute after one offence. Some examples from 2013 are as follows:

   - A pizza company was ordered to pay €4,000 for sending unsolicited marketing messages to customers without obtaining their consent. They had previously received a warning from the ODPC due to their failure to include an opt-out facility in all marketing communications with customers;
   - A car repairs company was ordered by the District Court to pay €2,000 to a charity, plus the ODPC's costs for the prosecution, due to their repeated failure to obtain the necessary consent from customers before sending marketing messages;

2. **Enforcement Notices Under Section 10 of the DP Acts**

   While the ODPC received over 900 complaints in 2013, most of these were resolved amicably without the need for a formal decision under section 10 of the DP Acts. There were, however, some enforcement notices and information notices served on companies. The key case involved a company that caused a data breach affecting nearly 1.5million people across Europe. This was Ireland's biggest and most significant data hacking breach to date. An Enforcement Notice was issued by the ODPC as part of a package of immediate actions undertaken by the ODPC to limit the effects of the data security breach. The Enforcement Notice required the company, amongst some other things, to notify all its clients and affected individuals about the security breach, to delete all personal data held for the purpose of providing services to its clients and to implement a series of changes to its procedures to bring them in line with industry best practices. The company was also not allowed process personal data until it had satisfied the ODPC that these requirements were being met. The ODPC then carried out a system-wide audit to examine the company's policies and procedures. Once the terms of the Enforcement Notice had been met, the ODPC lifted it.

3. **Information Notices Under Section 12 of the DP Acts**

   In 2013, just two companies were issued with Information Notices pursuant to section 12 of the DP Acts in order to assist the ODPC in carrying out their functions, such as to pursue an investigation.
4. **Damages Under Section 7 of the DP Acts**

Section 7 of the DP Acts allows an individual to sue for a breach of duty of care by a company where they can prove that a breach was caused by failure of the data controller. The 2013 case Collins v FBD Insurance plc [2013] IEHC 137, decided that in order for an individual to be awarded compensation under section 7 he or she must be able to prove that the breach caused him or her damage. In this case the Circuit Court had ordered an insurance company to pay the data subject €15,000 in compensation damages on the grounds that it had breached its duty of care to the data subject under the DP Acts. The High Court overturned the decision stating that in order for compensation to be awarded to a data subject under section 7 of the DP Acts, the data subject must establish that there has been a breach, that there has been damage and that the breach caused the damage. The claimant here had not successfully established that the breach caused her damage.

A recent Circuit Court decision awarded a woman €10,000 in damages against a pharmacy who had breached section 7 of the DP Acts. The claimant here did successfully establish that the breach caused her damage. The case demonstrates that where damage is proved, the courts are willing to award significant amounts of compensation.

5. **Director’s Liability Under Section 29 of the DP Acts**

Section 29 of the DP Acts provides for the prosecution of company directors where an offence by a company is proved to have been committed with the consent or connivance of, or to be attributable to any neglect on the part of the company directors or other officers. Two directors of a firm of private investigators were recently charged with twenty three counts of breaches of Section 29 for the role they played in the offences committed by the company. The company was charged with twenty three counts of breaches of Section 22 of the DP Acts for obtaining access to personal data without the prior authority of the data controller by whom the data is kept and disclosing the data to another person. The company was convicted on five sample charges and fined €1,500 per offence. The directors were convicted of one sample charge each and both were fined €1,500 for that offence. This is the first occasion on which company directors have been prosecuted by the ODPC for their part in the commission of data protection offences by their company.
Italy

Administrative Remedies

The Data Protection Authority (the “Authority”) has the power to investigate complaints and cases and to order the suspension of data processing (including transfer of data), as well as the destruction of data and other similar actions; these orders can be appealed to the courts.

The Authority can also impose administrative sanctions ranging between €3,000 and €300,000 depending on the type of data and violation involved. In particularly significant cases, e.g. when many data subjects are involved, the relevant amounts may be doubled.

Some amounts may be quadrupled if the amount of the applicable sanction is deemed to be insufficient for the violator because of its economic position.

Finally, the Authority may impose the publication of its decision in one or more daily newspapers, at violator’s cost and may also impose the block of the infringing database.

Civil Remedies

Individuals can file complaints with the Authority, and can seek compensation for monetary and also moral damages suffered as a consequence of violations of the privacy law.

Criminal Remedies

Imprisonment ranging between 3 months and 3 years depending on the type of violation. Note that criminal sanctions also apply in the case of unlawful data processing in relation to unsolicited marketing communications.

Imprisonment up to 2 years or (in case of subsequent compliance) fines equal to one/fourth of the maximum of the relevant administrative sanction for failure to adopt security measures.

The criminal decision will also be published in one or more daily newspapers, at the violator’s cost.

Other Remedies

Individuals within a data controller may be held jointly and severally liable for violations of the law, depending on the internal distribution of privacy tasks.

Selected Enforcement Actions/ General Comments

The Authority is fairly active in carrying out investigations and on-site audits. These may be initiated at the discretion of the Authority or triggered by complaints filed with the Authority by data subjects or interested third parties alleging a breach of privacy law.

On-site audits may be performed either at the legal offices or the business place of a company.

For the year 2014, the annual report of the Authority states that fines have been issued for a total amount of almost EUR 5 million, that almost 400 inspections have been carried out and replies of the Authority to claims have been almost 5,000.
The breaches sanctioned more often have been:

(i) failure to provide appropriate information to the data subjects;
(ii) breach of data security requirements and unlawful data processing;
(iii) breaches of orders and provisions of the Authority;
(iv) failure to disclose data breaches; and
(v) failure to comply with opt-out obligations in relation to marketing activities.

In addition, it should be mentioned the fact that the Authority is fairly active in taking part to international activities and joint initiatives organized with other European data protection authorities and also international authorities.

The annual report of the Authority is available in Italian on the Authority's website, at: www.garanteprivacy.it
Netherlands

Administrative Remedies
The Data Protection Authority has the power to investigate complaints and cases (both on its own initiative as well as on the basis of a complaint), and to order the suspension of processing and/or transfer of data, as well as the destruction of data and other similar actions including administrative orders on the pain of a financial penalty for each day that the controller fails to comply with the order; these orders can be appealed to the courts.

Failure to timely or correctly notify the Dutch Data Protection Authority of processing can be fined by a penalty of up to €4,500.

Civil Remedies
Individuals can file complaints with the Data Protection Authority, and can seek a judicial remedy for violations of the law.

The data controller is liable for damages (including immaterial damages) incurred by anyone as a result of any violation of the Data Protection Act committed by the controller or processor of the data.

Criminal Remedies
Infringement of notification obligations and/or in case of data transfers to countries of which the Dutch Minister has explicitly determined that transfers are prohibited, can qualify as criminal violation, subject to penalty fines not exceeding €8,100 where the violation is committed negligently and €20,250 or up to six months imprisonment in case of intentional infringement. Where the data controller is a legal entity, these amounts may be increased to €20,250 and €81,000 respectively;

Other Remedies
Under special circumstances, a director of the company may also be held liable.

There is also the risk of negative publicity for the violator.

Selected Enforcement Actions/ General Comments
Pending law reform:
An important legislative bill has been adopted recently and will enter into force per January 1st, 2016. The bill will introduce a statutory notification requirement in case of personal data breaches and expand the power of the Dutch Data Protection Authority (the "Authority") to impose considerably higher penalties. The background to the latter amendment entails the idea to provide the Authority further jurisdiction and more comprehensive measures to enforce compliance with the Dutch Personal Data Protection Act (the "Act").

The Authority will be allowed to impose penalties in case of non-compliance with the key legal requirements of the Act, such as the legal obligation to inform data subjects about the data controller's data processing activities. Penalties can run up as high as €810,000 or 10 (ten) percent of the company's annual turnover. Fortunately, in case of non-intentional violation of the Act, the Authority will be authorized to impose a penalty only after they have given the data controller the instruction and opportunity (under time limit) to correct the violation. The instruction requirement will not apply for
intentional non-compliance. In that event the Authority can impose a penalty immediately.

Some examples of recent enforcement action in the Netherlands include:

✓ In January 2015, several telecom providers communicated that they implemented new measures further to identified violations of the Dutch Data Protection Act (the providers retained personal data too long, after the purpose for the processing was no longer applicable). As a result, the Dutch Data Protection Authority decided not to take further enforcement actions.

✓ In December 2014 the Dutch Data Protection Authority communicated its intention to review the privacy terms of a social media company.

✓ In September 2014 the Dutch Data Protection Authority identified a company's violation of the Dutch Data Protection Authority as a result of its computer/tablet rental services to elementary schools. The tablets had built in apps that processed study results of the schools' students which were then used by the company for all kind of comparison purposes (in violation of the Act). According to the Authority, the company should have provided more/better information to the schools. The company has promised to mend its ways. The Authority will continue monitoring the actions of the company and will take further enforcement action in case of new identified violations.

✓ In July 2014 the Dutch Data Protection Authority and the Authority for Markets & Consumers concluded that the Netherlands Public Broadcasting violated the Dutch Data Protection Act by placing tracking cookies on the computers of website users, without their consent. The Netherlands Public Broadcasting promised to change their cookie policies accordingly, which they did after waiting too long. The Authority for Markets & Consumers imposed a € 25,000 penalty.

✓ In May 2014 the Dutch Data Protection Authority concluded that a company violated the Dutch Data Protection Act by placing tracking cookies on the computers of website users, without their consent.

✓ In January 2013, the Dutch Data Protection Authority and the Office of the Privacy Commissioner of Canada (OPC) have initiated a collaborative investigation into the processing of personal data by WhatsApp Inc. Users of Whatsapp do not have a choice to use the app without granting access to their entire address book (which contains phone number of users and non-users), which is in breach of Dutch and Canadian privacy laws. The coordinated investigation is a global first, as two national data protection authorities conducted their work together. In February 2014 the Dutch Data Protection Authority communicated that they may impose a remedial order on the pain of incremental penalty payments, if WhatsApp does not take remedial action itself. WhatsApp has taken remedial measures, but only partially. The issue has still not been fully resolved.

✓ In July 2012, it was concluded that a sickness absence management company processed sensitive personal data (health) in breach with the principle of proportionality and without sufficient legal basis. The sickness absence management company was ordered to destroy all personal data and inform the data subjects of their legal rights, subject to a penalty.

✓ GVB, a public transportation company that had stored the travel data of students (on a chip card) for an
unreasonable long period, was ordered to implement specific retention periods for the processing of the personal data and to destroy or anonymize the data on the last day of that retention period, subject to an incremental penalty of €5,000 per administrative measure and for each week (or part thereof) that they did fully not implement the measures imposed by the Dutch Data Protection Authority up to a maximum of €250,000 per measure.

In January 2011, the Dutch Data Protection Authority concluded that the municipality of Charlois illegitimately processed data with regard to someone's race for the purpose of maintaining a public order. The Authority imposed an order to cease the processing of racial data within three days and delete these data from the database within three months, subject to an incremental penalty of €2,000 per measure and for each day that the municipality of Charlois did not satisfy the order up to a maximum of €250,000 per measure.

Transfer of personal data to US/Australia: The Data Protection Authority held that there was not an adequate level of protection to transfer personal data from a black list to police authorities in third countries. Transfer was not allowed.

An internet search engine company fined €15 million for violating Dutch data protection laws.
Norway

Administrative Remedies
The Data Protection Authority has the power to investigate complaints and other cases on its own initiative. In case of any privacy law breaches, the DPA may order to cease unlawful processing and impose coercive fines for non-compliance with such orders.

Furthermore, for privacy law breaches, the DPA may impose a regulatory fine at a maximum of 10 times the national insurance basic amount, which at present corresponds to about €110,000.

Civil Remedies
A data controller may be liable to compensate the data subject for any damage suffered, including pecuniary and non-pecuniary damages.

Criminal Remedies
Fines of unspecified value, as well as imprisonment which may be for a term not exceeding one year.

Other Remedies
Sanctions may also be directed towards responsible directors and employees.

Selected Enforcement Actions/ General Comments
Some examples of recent case law and enforcement action in the Norway include:

- In August 2014, Pixima was imposed an administrative fine of NOK 75,000 (about € 9,000) for illegal data processing. The company assisted various petrol stations by collecting data from video footage in order to identify customers that had not paid for the petrol. However, Pixima, acting as a data processor for the data controller petrol stations, went beyond the agreement with the petrol stations, and established their own archive over non-paying customers. Further, the agreements with the petrol stations did not satisfy the minimum criteria in the Personal Data Act, nor were the data sufficiently protected with a sufficient degree of security. The data was also kept indefinitely, in violation of the requirement to delete when no longer relevant.

- In January 2014, the security company Securitas was imposed an administrative fine of NOK 75,000 (about € 9,000). Securitas did not have satisfactory risk evaluations in place for of its processing of personal data, nor satisfactory measures to secure data. Finally, the data processing wording in the agreements with the customers was not satisfactory.
Poland

**Administrative Remedies**

The Inspector General of Data Protection ("Inspector General") has the power to investigate any complaints and cases. In case of any breach of the data protection law (DPL), the Inspector General may order to restore the proper legal state, and in particular: to remedy the negligence; to complete, update, correct, disclose or not to disclose personal data; to apply additional measures protecting the collected personal data; to suspend the flow of personal data to a third country; to secure personal data, or to transfer it to other subjects; and to delete the personal data.

These orders can be appealed to the courts.

In case of non-compliance with the decisions, the Inspector General may impose administrative penalties/fines in order to enforce them – in case of repeated non-compliance up to 50,000 PLN (approx. €12,000) with respect to an individual or up to 200,000 PLN (approx. €47,600) with respect to an entity.

**Civil Remedies**

Individuals may file actions in court (in particular request damages caused by infringement of privacy).

**Criminal Remedies**

Fines of up to 1,080,000 PLN (approx. €257,000); restriction of liberty and imprisonment of up to 3 years.

Additionally DPL provides that a person who prevents or impedes an inspector in execution of its control activity will be subject to a fine, restriction of liberty or imprisonment of up to 2 years.

**Other Remedies**

Corporate officers and in some cases, employees of the data controller may face personal criminal liability.

**Selected Enforcement Actions/ General Comments**

Some examples of recent enforcement action in Poland include:

- In 2013 the Inspector General submitted 16 motions to the public prosecutor for the institution of criminal proceedings (there were 12 motions in 2012, 10 in 2011, 23 in 2010)

- In 2013 the Inspector General conducted 318 audits and monitored 338 IT systems (in which personal data are processed). In the said year there were 1879 complaints submitted related to breach of personal data law, in particular relate to public administration, finance and marketing areas.
## Portugal

### Administrative Remedies
The Data Protection Authority (the “Authority”) has the power to investigate complaints and cases, and to order the suspension of processing and/or transfer of data, as well as the destruction of data and other similar actions including administrative fines; these orders can be appealed to the courts.

### Civil Remedies
Individuals can file complaints with the Authority, and can seek a judicial remedy for violations of the law.

### Criminal Remedies
Fines ranging between €250,00 and €2,500,00 for natural persons, and fines between €1,500.00 and €15,000.00 for entities; and imprisonment of up to 1 year or an equivalent monetary fine.

The above fines may be increased to double the amount [i.e. €500 up to €5,000 in the case of natural persons and €3,000 up to €30,000 for entities] if it concerns sensitive data. In this case, it is also possible to be subject to imprisonment of up to 2 years or an equivalent monetary fine.

### Other Remedies
Directors and individuals within a company may face legal sanction.

### Selected Enforcement Actions/ General Comments
Some examples of recent enforcement action in Portugal:

- Fines have been imposed for various activities; however the most common ones concern the capture of images (CCTV) without prior authorization from the Portuguese Data Protection Authority.

- The Portuguese Data Protection Authority has applied a fine of €7,000.00 (the Portuguese Criminal Court of Porto considered the application of an admonition as sufficient), where data was collected without prior notification and communicated to third parties.

Another decision which concerned the disclosure by a legal person on the Internet of an image and credit information of a natural person, without authorization, resulted with a fine of €1,500.00 for breaching the requirement to notify the Portuguese Data Protection Authority.
Slovakia

Administrative Remedies
The Slovak Data Protection Office ("the Office") has the power to investigate complaints and cases, and to impose penalties for breaches of the data protection act; penalties can be up to €200,000 and it can be imposed repeatedly if the same breach is also committed repeatedly, but also for the same breach if the sanctioned person does not remedy the breach within the deadline stipulated by the Office.

Liability for a particular breach ceases to exist if the Office fails to impose a penalty within two years from the date on which the Office learned about the breach, however no later than five years from the date of the breach.

Civil Remedies
Indians can seek judicial remedies and damages for breach of protection of their personhood.

Criminal Remedies
An individual found guilty of the unauthorized disposal of personal data may be punished by imprisonment for a term of up to 2 years.

Other Remedies
None.

Selected Enforcement Actions/ General Comments
Data controller was imposed a fine of € 5,000 for not informing data subjects of the fact that processing of their personal data was entrusted to a data processor.

Data controller was imposed a fine of € 4,945 for not completing the security project concerning the terms of data processing in the information system.

In cases when cooperation was not provided in an administrative proceeding, the Office often imposed a fine ranging from €1,500 to €9,000.

In the course of inspection activities, the Data Protection Office focused mainly on prevention. In the years 2011-2012, the Office imposed fines of € 26,850 in total.
Spain

Administrative Remedies

The Spanish Data Protection Agency (SDPA) has the power to initiate inspections ex officio, investigate complaints and conduct sectoral investigations, and initiate sanctioning administrative proceedings that might end up with a fine being imposed. The SDPA can also order the suspension of processing and/or transfer of data, as well as the destruction of data and other similar actions in the event of very serious infringements or infringement of fundamental rights.

The resolutions of the SPDA may be appealed to the Spanish National Court.

Fines for minor infringements range between €900 and €40,000; for serious infringements between €40,001 and €300,000; and very serious infringements €300,001 and €600,000.

Within the relevant range of fines, the amount can be increased or reduced depending on the damages caused, the benefit obtained, the level of intentionality, etc.

The SDPA may, “on an exceptional basis”, put the commencement of the sanctioning administrative proceedings on hold and issue a warning to the offender and require evidence of corrective measures within a given deadline, subject however, to the following criteria being met:

(i) The facts must constitute a minor or serious infringement under the Spanish data protection Act (Act); and
(ii) The offender has not been previously sanctioned or warned.

Likewise, under a literal construction of the Act, the “warning system” is arguably configured as “optional” for the SDPA and it would be difficult to argue that a company has an enforceable right to be “warned” (instead of fined), even if the required conditions to be “warned” are satisfied.

Civil Remedies

Individuals can bring a civil action to court in order to obtain compensation for damages arising out of personal data infringements. The amount to be imposed by the courts would depend on the seriousness of the rights infringed and the damages suffered by individuals. Individuals have to prove or evidence the effective harm caused.

Also, a data protection infringement may sometimes entail damages for breach of image, intimacy or honor fundamental rights following a specific civil proceeding for violation of such fundamental rights.

Criminal Remedies

Neither Spanish data protection laws and regulations nor the Spanish Criminal Code specifically foresee any criminal liability linked to a breach of personal data protection laws.

However, the Criminal Code provides that, anyone who violates the privacy of a third party in order to discover secrets or, without the third party’s consent, seizes his/her papers, letters, email messages, any other documents or personal belongings, or intercept his/her transmissions or uses technical devices to listen to, transmit, record or reproduce sound or images, or any other communication signal, shall be punished with imprisonment penalties ranging from 1 to 4 years.
and daily fines ranging between 12 and 24 months.

Similar penalties apply to those who, without being authorized, use, modify, etc. a third party’s personal or familiar data registered in a file. Such fines would be increased if the violation relates to sensitive data (ideology, religion, beliefs, health, racial origin, sexual preferences or relates to minors).

Eventually, although we have not seen it in practice, it may not be totally discarded that a very serious infringement carried out with a high degree of intentionality may be considered as falling within the aforementioned criminal infringements.

Other Remedies

N/A

Selected Enforcement Actions/ General Comments

Fines have been imposed for various activities, including, but not limited to: deceptive or fraudulent data collection; failure to inform data subjects; transfer of data without consent; transfer between companies in a group without consent; data leaks on the Internet; sending unsolicited advertising and emails without consent; and non-compliance with destruction of media containing personal data.

Some examples of recent enforcement action in Spain include:

✓ In 2009, a telephony operator was fined €420,000 for unlawful disclosure of data to debt recovery companies;
✓ In 2007, a television production company was fined €1.08M for leaking personal data via the Internet, and related violations;
✓ In 2012, an asset solvency services company was fined €50,000 for failing to inform data subjects of processing;
✓ Between 2008 and 2011, several companies were fined €300,000 for transferring personal data without consent;
✓ In 2010, a telecommunications company was fined €40,000 for international data transfer between companies in a group without consent;
✓ Since 2003, several fines of €30,000 were imposed for sending unsolicited advertising without respecting the data subjects’ right to cancel.

More recently, the SDPA has adopted a more discreet approach to administrative sanctions and is usually imposing the lowest possible fine of each category (minor, serious, very serious) unless the infringement was intentional or caused by data controller's gross negligence. In this regard, see some examples of recent (in 2014) key cases below:

✓ Two companies fined €3,000 for using cookies on their websites in breach of the applicable cookies rules.
✓ Company fined €1,500 for a minor infringement concerning the duty to inform upon data collection through a website contact form.
- Company fined €40,000 for a serious infringement related to employee health data.
- Company acting as data processor fined €6,000 for breaching the consent rule while engaging in marketing on behalf of a supply company (the data controller) without duly obtaining the consent of the covered customers.
Sweden

**Administrative Remedies**

The Data Protection Authority has the power to carry out inspections (including gaining access to i) the personal data being processed, ii) property in which personal data is stored and iii) any documents relating to the processing and safeguarding of personal data) as well as to investigate complaints and cases, and to order the suspension of, inter alia, processing and/or transfer of data, as well as the destruction of data and other similar actions; these orders can be appealed to the Swedish county administrative court.

Some of the Data Protection Authority’s decisions in this respect are sanctioned with fines (up to SEK 1,000,000) (approximately USD 116,000), should the data controller not comply with the decisions or not provide the Data Protection Authority with the relevant information referred to above.

**Civil Remedies**

Individuals can file complaints with the Authority, and can seek a judicial remedy (damages) in Swedish courts for violations of the law.

**Criminal Remedies**

A person may be fined (unspecified value) or, in very severe cases, be imprisoned between 6 months and 2 years depending on the violation.

Criminal liability falls on the person responsible at the data controller who is guilty of committing the breach, normally the board of directors.

The size of the fine is not fixed and depends on, inter alia, how serious the violations are and the size of the income of the persons subject to the fine in question. According to the Criminal Code, the fine will normally not be lower than SEK 200 (approximately USD 23) and not higher than SEK 150,000 (approximately USD 17,500).

**Other Remedies**

The right for the data subjects to request correction and deletion of unlawfully processed personal data.
Selected Enforcement Actions/ General Comments

There is limited case law in Sweden related to breach of the data privacy regulation.

Some examples of recent enforcement action in Sweden include:

- Four real estate companies in the Swedish municipality of Gothenburg were fined SEK 20,000 (approximately USD 2,300) each for unlawfully processing sensitive personal data about their tenants. No individual was fined.

- A board member of a school was convicted for disclosing health-related personal data belonging to an employee of the school on the school’s webpage. The person committing the crime was fined SEK 40,000 (approximately USD 4,600).

- Two different credit companies were instructed to cease their processing of personal data as it was considered to be in breach of Swedish law not to inform individuals that they had been subject to credit checks. In both cases, it was sanctioned with a SEK 1,000,000 (approximately USD 116,000).

The amounts of damages to data subjects vary but are normally within the range of SEK 5,000-60,000 (approximately USD 580-7,000) in relation to each data subject. Most cases involving private companies relate to unpermitted disclosure of personal data on the Internet.
Switzerland

Administrative Remedies

The Federal Data Protection and Information Commissioner has the power to conduct investigations, as well as to issue recommendations (i) if the data processing concerned violates a large number of persons; (ii) data collections must be registered or (iii) if there is an information obligation in accordance with the Data Protection Act.

Civil Remedies

Violating data protection obligations may result in civil liability. The violated person may sue the violating person for correction, cease and desist, deletion and damages covering financial losses or lost profits incurred by the violated person. The damages depend on the actual losses and lost profits proved by the plaintiff.

In exceptional cases, the violating party may have the obligation to pay a satisfaction amount to the data subject to compensate for immaterial damages.

Criminal Remedies

Fines of up to CHF 10'000, and imprisonment for up to three years for violations of professional secrecy. However, not every violation of a data protection obligation automatically results in a sanction provided for in the Data Protection Act. Only the following violations by private persons are subject to penal sanctions and a fine:

- Failing intentionally to comply with access rights or information obligations;
- Failing intentionally to register accurately their data collections or to notify the Federal Data Protection and Information Commissioner of the safeguards implemented for the cross-border transfer of personal data to countries that do not provide an adequate level of protection;
- Failing intentionally to cooperate in investigations by the Federal Data Protection and Information Commissioner or providing inaccurate information;
- Disclosing intentionally and without authorization confidential and particularly sensitive information or personality profiles obtained in a professional function that requires the knowledge of such data or while working for a third party subject to confidentiality obligations.

Other Remedies

The individual committing the breach will be subject to the sanctions. However, also the directors and board members of a legal entity may be subject to sanctions.
Previously, the Federal Data Protection and Information Commissioner emphasized its consultative and administrative role.

Since recent privacy developments it appears the Federal Data and Information Commissioner is taking a more proactive approach in pursuing data processing that may potentially violate the privacy rights of a wider population. It is expected that the number of court cases will rise in the future as a result of this approach.

To date, no fines have been imposed in published case law. Please note that first instance case law is usually not published and second instance is only published occasionally. Third instance case law is published on a regular basis.

While no fines were imposed, there have been some notable decisions enforcing data privacy rules:

**Judgment of the Swiss Federal Supreme Court on Logistep (BGE 136 II 508, September 8, 2010)**

Acting on behalf of rights holders, Logistep had been collecting the IP addresses of users who were using Peer-to-Peer networks in order to exchange what was purported to be illegal uploads of copyrighted material, such as video and music files. Once they were in possession of the IP addresses, rights holders filed criminal charges which allowed them to identify the persons involved and to claim damages from them. The Swiss Federal Supreme Court ordered Logistep to halt all copyright-related data processing activities and banned it from forwarding any data already collected to copyright holders. The key arguments of the Swiss Federal Supreme Court can be summarized as follows:

- In the case of a data transfer, if the recipient is able to identify the person concerned, the data shall be considered personal. If personal data is involved, the Data Protection Act must apply to all processing activities involving this data.

- In the abstract, it is impossible to determine whether IP addresses, in particular dynamic ones, involve personal data or not. However, IP addresses are considered to be personal data if, based on common experience, third parties who are interested in identifying the individual user can be expected to undertake the effort to make such identification. This was true in the case of Logistep, since its entire business model was premised on the identification of the individual user.

- In processing the data it had collected, Logistep had violated the principles of purpose limitation and transparency. The issue to be decided was whether the company had provided any legal justification for its actions. In the court’s opinion, a strictly systematic interpretation according to which a legal justification can only be invoked for the cases covered by paragraphs b) and c), but not a) of Article 12.2 of the Data Protection Act is not admissible, for even though the current version of sub-paragraph a) no longer refers to justificatory grounds, it does not explicitly exclude them either. The provision must therefore be interpreted in such a way that a justification for the processing of personal data in violation of the principles set out in Article 4, Article 5 paragraph 1 and Article 7 paragraph 1 of the FADP cannot as a general rule be excluded; however in this specific case, justificatory grounds may only be accepted with the greatest restraint.

- The Supreme Court made it clear that it did not consider that data protection must always take precedence over copyright protection. In its opinion, it is the task of the legislator, and not the judge, to ensure that the appropriate
steps are taken to guarantee copyright protection when works are distributed via the new technologies.

Moneyhouse-Case

✓ The operator of moneyhouse.ch, itonex AG in Rotkreuz, offers a contact search service, which involves the publication of address data on the Internet regardless of consent of the relevant persons. Numerous individuals thereupon approached the Federal Data Protection and Information Commissioner which then initiated a clarification of facts and demanded from itonex AG to take the people search function off the Internet. The company did not react to that request, whereupon FDIPC took legal action before the Federal Administrative Court and requested to immediately enjoin the people search service as an immediately enforceable injunction, i.e. without any prior hearing of the opposing party. The Federal Administrative Court complied with the request. In accordance with the Federal Data Protection and Information Commissioner’s demands, it additionally obliged itonex AG to instruct the operators of Internet search engines to delete saved address data immediately. After the hearing of itonex AG, the Federal Administrative Court annulled the immediately enforceable injunction, leading to the personal data being accessible again on the website of moneyhouse.ch. In February 2013, itonex AG has come to an arrangement regarding the handling of personal data with the Federal Data Protection and Information Commissioner and observes the negotiated recommendations, such as, e.g.: Addresses which itonex AG obtained from an individual will only be published on moneyhouse.ch if a justification exists. Only if the person concerned consents to his or her current address being accessible over the Internet without any particular proof of interest is that consent considered a sufficient justification. In case of a justification other than the person’s consent, itonex AG needs to ensure for the other processing of the address data that the address exclusively serves authorized persons for the verification of the identity of the person concerned. Furthermore, the persons concerned have a right to address a personal information request as well as the possibility to request deletion. With regard to company information, such information is based on the commercial register, a summary thereof can be found on zefix.ch. All data published on moneyhouse.ch is public and may be published with no time limit. The consent of the person or company concerned is not required. FDIPC has now again sued moneyhouse.ch before the Federal Administrative Court because he believes that moneyhouse.ch has only partially implemented his recommendations. A decision is pending.

BGE 138 II 346, May 31, 2012
United Kingdom

**Administrative Remedies**

The UK authority (the Information Commissioner’s Office or ICO) has the power to investigate complaints and cases, to order the suspension of processing, and to take other actions including information and enforcement notices.

Since April 2010, the ICO has had the power to impose fines up to £500,000 for serious breaches of the Data Protection Act 1998 (“DPA 1998”), where the contravention is likely to cause substantial damage or distress and either the contravention was deliberate or the data controller knew or ought to have known that there was a risk that this serious contravention would occur and failed to take reasonable steps to prevent it. In May 2011, the power to fine was extended to serious breaches of the Privacy and Electronic Communications Regulations. The notice imposing the fine is published on ICO’s website.

**Civil Remedies**

Individuals can file complaints with ICO. The DPA 1998 also gives the individual a limited right to compensation for damage caused by a breach. Individuals are also able to obtain a court order for rectification, blocking, erasure or destruction of inaccurate data.

**Criminal Remedies**

In a few cases, breach of the DPA 1998 can constitute a criminal offence, for example, breach of the obligation to notify or failure to comply with information and enforcement notices.

The knowing or reckless obtaining or disclosure of personal data without consent of the data controller is, subject to certain defenses, an offence, as is offering to sell data so obtained or disclosed. Officers of companies which have committed an offence may also be liable to prosecution. Offenders are potentially liable to an unlimited fine.

**Other Remedies**

Frequently, ICO will resolve cases by accepting undertakings not to commit further breaches.

**Selected Enforcement Actions/ General Comments**

ICO publishes its enforcement activity on its website at https://ico.org.uk/action-weve-taken/enforcement/. Here are some recent examples:

**6 January 2015**

A green deal energy company, was prosecuted for failing to respond to an information notice. The company was fined £5000.

**5 November 2014**

A hotel booking website was fined £7,500 following a serious data breach where a vulnerability on the company’s site allowed attackers to access the full payment card details of 3,814 customers.
23 July 2014
An online travel services company, was fined £150,000 after a serious breach of the Data Protection Act revealed thousands of people’s details to a malicious hacker.

16 December 2013
A fine of £175,000 was imposed on a pay day loans company for sending millions of spam text messages.

5 August 2013
A fine of £75,000 was imposed on the Bank of Scotland after customers’ account details were repeatedly faxed to the wrong recipients. The information included pay slips, bank statements, account details and mortgage applications, along with customers’ names, addresses, and contact details.

24 January 2013
A fine of £250,000 was imposed on a global consumer products company after its online service was hacked in April 2011, compromising the personal information of millions of customers, including their names, addresses, email addresses, dates of birth, account passwords, and potentially payment card details.
Asia Pacific
The Privacy Act 1988 (Cth) provides for complaints driven investigations as well as granting powers to the Privacy Commissioner to investigate a matter on its own initiative. If a complaint is found to be substantiated by the Commissioner, the Commissioner may order that compensation be paid to the individual (and/or that the organization ceases particular conduct or undertakes a particular act, e.g. issues a public statement, apologizes, etc.).

Determinations of the Commissioner are, however, not binding or conclusive between the parties. Where a matter originated from an individual's complaint, either the individual or Commissioner must apply to the Court to enforce the Commissioner's determination. If the matter originated from the Commissioner's own investigation, only the Commissioner can apply to the Court for enforcement of its determination.

As of March 2014, new civil penalty provisions have been included in the Act under which an individual can be fined a maximum of $360,000 and a body corporate a maximum of $1,800,000, if it seriously or repeatedly interferes with the privacy of an individual.

Interference with the privacy of an individual in this context will only be found in the limited circumstances set out in section 13 of the Privacy Act. These circumstances include:

1. Breaches of an Australian Privacy Principle (APP) or an approved APP code in relation to personal information about the individual;
2. Breaches of the credit reporting provisions of the Act in relation to personal information or a registered CR Code or requirements in relation to tax file numbers of an individual;
3. Breaches by Commonwealth contracted service providers of contractual obligations in relation to personal information; and

There are no criminal remedies (with some specific exceptions, e.g. in relation to breaches of the privacy provisions in the Telecommunications Act 1997 (Cth)).

Amendments to the Privacy Act came into effect on 12 March 2014, including expanded enforcement powers for the Privacy Commissioner and civil penalties of up to AU$360,000 for individuals and AU$1.8 million for corporations (as noted above). However, as of 15 July 2015 there have not yet been any fines issued under the amended laws, possibly due to the time lag between alleged breaches and the pace of investigations by the Privacy Commissioner. Therefore the cases outlined below relate to breaches of the Privacy Act and enforcement mechanisms in place prior to March 2014.
In its 2013-14 Annual Report, the Office of the Australian Information Commissioner (OAIC) reported that 59 monetary awards were issued, the quantities being:

- Awards of less than A$1,000 were made to 14 individuals;
- Awards of between A$1,000-$5,000 were made to 18 individuals;
- Awards of between A$5,000-$10,000 were made to 9 individuals; and
- Awards of over A$10,000 were made to 8 individuals.

We have also outlined below some recent findings reported by the OAIC.

**Department of Immigration and Border Protection (DIBP)**

The DIBP breached IPPs 4 and 11 of the Privacy Act for failing to put in place reasonable security safeguards to protect the personal information it held, for unlawfully handling personal information and for unlawfully disclosing personal information of approximately 9250 asylum seekers in a report made available on its website for eight and a half days in February 2014. The personal information disclosed in the report included personal details, information relating to their immigration into Australia and why the particular asylum seeker was deemed unlawful.

The Privacy Commissioner was satisfied that the DIBP’s responses to the breach would strengthen its privacy framework and ensure compliance with the Privacy Act. It therefore merely recommended that DIBP monitor its internal compliance with its new processes to ensure continued compliance with the Privacy Act.

**Cupid Media Pty Ltd (Cupid)**

Cupid, which operates online dating websites, was found in breach of NPP 4 of the Privacy Act for failing to take reasonable steps to secure the personal information of over 250,000 customers which it held online. The investigation, with which Cupid cooperated, found that a data breach resulted in Cupid customer records and personal information being stolen and found on a third party server operated by hackers. Cupid was found to have failed to take reasonable steps to protect its customers’ personal information from misuse, loss and unauthorised access, modification and disclosure, and also to have failed to destroy the relevant information after it was no longer needed.

Following the breach, Cupid undertook extensive privacy and data security programs designed to ensure compliance with the Privacy Act. The Privacy Commissioner’s recommendation was limited to the requirement that Cupid regularly review its privacy and data security processes to ensure compliance with the Privacy Act and best practice.

**Telstra**

Telstra is Australia’s largest provider of telecommunication services, and is responsible for the publication of the Australian telephone number directory. The Privacy Commissioner determined that Telstra breached NPP 1.3 of the Privacy Act by failing to inform a judge that his name and address would be published in a telephone directory, after he contacted Telstra requesting the installation of a phone line to be connected to his home alarm system. Specifically,
Telstra was in breach for failing to take reasonable steps to notify the judge of the reasons for its collection of his personal information and possible disclosure of that information.

The Privacy Commissioner declared that Telstra:

✓ pay $18,000 to the complainant for non-economic loss to the complainant’s privacy;
✓ apologise in writing;
✓ review its processes to ensure customers are notified of the possible disclosure of their personal information and given the opportunity to opt out of such disclosure; and
✓ review its Privacy Statement to reference the collection of information for the purpose of publication.

Pound Road Medical Centre (PRMC)

The Privacy Commissioner determined that PRMC was in breach of NPP 4 of the Privacy Act in late 2013 for failing to take reasonable steps to secure sensitive medical records of approximately 960 patients from misuse, loss, unauthorised access, modification or disclosure. Further, PRMC was found in breach for failing to destroy or de-identify the personal information it held after such information was no longer needed by PRMC. The records were kept in a locked garden shed at a location no longer used by PRMC, which was deemed to be an insecure temporary structure unsuitable for the storage of sensitive records and personal information.

The Privacy Commissioner recommended that PRMC undertake a risk assessment with respect to privacy practices and develop a data breach response plan to ensure it meets its obligations under the Privacy Act.

Telstra and Mr Ben Grubb

A journalist named Ben Grubb contacted Telstra claiming a right of access under the Privacy Act to ‘all the metadata information Telstra has stored’ about him in relation to his mobile phone service. Telstra refused to provide the information, and Grubb lodged a complaint with the OAIC claiming that Telstra had breached his rights under the Act. The request was narrowed down to “network data” (IP addresses, URL information, and cell tower location information) and incoming call records - specifically, inbound call numbers. The key questions for the Commissioner were:

(a) whether the complainant's metadata held by Telstra constitutes "personal information"; and if so,

(b) whether it was improperly withheld in breach of NPP 6.1.

The Commissioner held that given Telstra's size and resources available to it, Telstra did and could associate network data with the complainant's identity and this data was therefore personal information.

The inbound call numbers were also personal information "about" the complainant but also contained personal information of the callers. An exception to the obligation to provide personal information applies where providing access would have an unreasonable impact upon the privacy of other individuals. If a person unintentionally called the
complainant, revealing that person's personal information to the complainant as part of the incoming call records would be an interference with that person's privacy.

It was not possible for Telstra to identify whether customers contacted the complainant intentionally or unintentionally, and there was no way for Telstra to edit the information to provide only the numbers of those individuals who intentionally contacted the complainant. Consequently, Telstra could refuse access to all of the inbound call numbers.
China (PRC)

**Administrative Remedies**

China has yet to promulgate a specific and standalone privacy or data protection law. However, pursuant to the amended Law of the PRC on the Protection of Consumer Rights and Interests (which came into effect in March 2014), business operators which provide goods or services to PRC consumers, among other things: i) should adopt the principles of legality, legitimacy and necessity in their collection and use of consumers’ personal data; ii) should explicitly inform the consumers the purposes, scope and manner of data collection and use and obtain their consent to the same; iii) should disclose its personal data collection and use practices and must not collect or use the personal data of consumers in contrary to any laws or regulations or beyond the scope as agreed with the consumers; iv) must keep the consumers’ personal data strictly confidential, and must not disclose, sell or unlawfully provide the same to a third party; v) should adopt technical and other necessary measures to ensure that the personal data is secure and to prevent data leakage or loss; vi) should take remedial steps at once where data leakage or loss occurs; vi) must only send commercial messages to consumers with their consent or at their request, or where they have not expressly declined the receipt of the same.

If a business operator violates the above provisions and infringes upon the personal information of consumers, the State Administration for Industry and Commerce or its local counterparts may issue a warning, confiscate illegal income, impose a fine of not less than once but not more than 10 times the illegal income, and/or the imposition of a fine of not more than RMB500,000 (approximately USD83,000) if there is no illegal income. In serious circumstances, the business operator will be ordered to cease business and reorganize, and its business licence will be revoked.

**Civil Remedies**

Individuals may bring a civil claim for monetary damages for any harm suffered, and may also demand an apology from the offender.

Under China’s Tortious Liability Law (which came into effect on 1 July 2010), violation of another’s “civil rights and interests” would give rise to tortious liability and privacy rights are expressly listed as a form of civil rights and interests.

**Criminal Remedies**

The PRC Criminal Code makes it an offence for individuals working in financial institutions, telecommunications companies, transportation companies, educational institutions, medical institutions, or government organizations who sell or illegally provide personal information collected during the course of work or provision of services. Offenders may be detained or jailed for not more than 3 years. and/or fined. Individuals stealing or illegally obtaining such information will be subject to the same penalties in serious cases. Where an organisation commits the above offences, it will be subject to a penalty and its officers who are directly responsible for this will be subject to the penalties that are applicable to individual offenders as discussed above. Recently, there are proposed amendments to these provisions: i) the offence of sale or illegal provision of personal data will be applicable to all industries across the board (instead of the 6 designated industries); b) introducing a new offence: anyone selling or illegally providing personal information of an individual to a third party without the individual's consent will be subject to detention or imprisonment for not more than 2 years, and/or imposition of a fine. Note such proposed amendments have not been passed yet.
Other Remedies

Selected Enforcement Actions/ General Comments

The authorities have stepped up their efforts in enforcing the laws in relation to the sale of personal data and the sensitivity regarding the use of personal data continues to increase from prior years. Further, the authorities are keen to combat the practice of “doxing” (i.e. Internet users banding together to expose an individual to public humiliation by disclosing the individual’s personal information or “private affairs”) which has become very common in China in recent years. One example is the passage of the Provisions of the Supreme People’s Court on Several Issues concerning the Application of the Rules Regarding Cases of the Infringement of Personal Rights over Information Networks which came into effect in October 2014. The Provisions expressly prohibit “doxing” but may be read to apply more broadly to the online disclosure of personal information on the Internet in general.
Hong Kong

**Administrative Remedies**

The Privacy Commissioner ("PCO") has the power to conduct investigations, inspect data privacy systems, issue enforcement notices and submit matters to the police for criminal investigation or prosecution.

**Civil Remedies**

Individuals can file complaints with the PCO for investigation and civil claims in the court.

Individuals who have suffered harm from a contravention of Hong Kong data protection law may apply to the PCO for legal assistance in obtaining information and/or pursuing claims against data users.

**Criminal Remedies**

Fines of up to HK$1,000,000 and up to 5 years imprisonment for direct marketing offences.

Failure to comply with an enforcement notice issued by the PCO is punishable by a fine of up to HK$50,000 and up to 2 year imprisonment (with fines of up to HK$100,000 and up to 2 years imprisonment for recalcitrant behaviour). Continuing non-compliance attracts a daily penalty of up to HK$1,000 (or HK$2,000 for recalcitrant behaviour).

**Other Remedies**

Private prosecution; damages for injury to feelings.

**Selected Enforcement Actions/ General Comments**

Here are some examples of recent enforcement action in Hong Kong:

- In 2010, the PCO investigated Octopus Rewards Limited for sale of personal data of over 2 million customers. The sale of personal data without the consent of the data subject be was made a criminal offence under the Personal Data (Privacy) (Amendment) Ordinance, which came into force in 2012.

- The amended Personal Data (Privacy) Ordinance dramatically increases penalties and introduce new offences particularly focused on direct marketing and unauthorized disclosure of personal data.

- In 2012, the PCO also investigated various local retailers in relation to their collection and use of customer personal data in connection with customer loyalty programs. The PCO required the retailers to cease collecting customers’ Hong Kong identity card numbers, delete any such data already collected, and give more comprehensive notifications to customers upon the collection of their personal data.

- In 2014, the PCO conducted a survey of 60 popular mobile applications developed by Hong Kong entities and found that their transparency in terms of privacy policy was clearly inadequate and there was no noticeable improvement compared with the results of a similar survey conducted in 2013. The PCO has also issued a warning and enforcement notice against 2 mobile application operators for inadequate protection and excessive collection of personal data.
Indonesia

Administrative Remedies

1. Governmental Civil Officials (i.e. the Ministry of Communication and Informatics officials) have the power to investigate complaints and determine violations of data privacy/protection.

2. Under Government Regulation No. 82 of 2012 on the Implementation of Electronic Systems and Transactions (“GR 82”), any violations of provisions of GR82 are subject to the following administrative sanctions:

3. Warning letters;

4. Administrative fines;

5. Suspension; and

6. Deregistration.

GR 82 also provides that a written notification to the relevant data owner is required if there is a breach. However, GR 82 is silent on when the notification should be made.

Civil Remedies

The Law No. 11 of 2008 on Electronic Information and Transactions (“EIT Law”) stipulates that individuals whose rights have been violated can file lawsuits to the relevant courts.

Criminal Remedies

Under Article 32 of the EIT Law:

1. Each person is prohibited from intentionally and unlawfully changing, adding, reducing, transmitting, destroying, causing to disappear, transferring and hiding in any way electronic information and/or electronic documents belonging to other persons or the public;

2. Each person is prohibited from intentionally and unlawfully moving or transferring electronic information and/or electronic documents to another person; and

3. Each person is prohibited intentionally or unlawfully from committing the action referred to in sentence (1) that causes confidential electronic information and/or electronic documents to become accessible by the public which changes the data from the original.

Violation of the above provision can be subject to imprisonment for up to 10 years and/or monetary fines of up to five billion Rupiah (approx. €400,000).

Other than the EIT Law, Article 322.1 of the Indonesian Criminal Code also provides that anyone who intentionally discloses confidential information that he/she is under an obligation to keep secret by virtue of his/her present or past position of employment is subject to imprisonment of nine months.

The Indonesian Police is the authorized official which holds the rights to investigate the above actions.
There are no specific laws and regulations in Indonesia that govern data privacy/protection. The main law and regulation in Indonesia that address data privacy/protection are as follows:

1. The EIT Law which was enacted on 21 April 2008; and
2. GR 82 which was enacted on 15 October 2012.

Implementation of the law and regulation

Indonesia is an emerging market and as a civil law country its laws and regulations are principle based, where implementation is driven by policy. Therefore, the implementation of the EIT Law and GR 82 may depend on the practical approach given the nature of electronic/internet development which is likely to be more advanced than what is regulated.

Enforcement of data privacy/protection clauses has not yet been tested in Indonesian courts. There has been no court case reported in relation to breaches of data privacy/protection.

Requirement for Consent

In principle, unless a law or regulation provides otherwise, the EIT Law requires the consent of the individuals concerned to collect, use and utilize their private or personal information through electronic media.

GR 82 further requires that the use or utilization of personal information must be in accordance with the purpose conveyed to the personal data owner for the data collection.

Draft Regulations

The Government has been preparing draft implementing regulations in relation to data privacy protection which may come into force this year.
## Japan

### Administrative Remedies
The competent ministry (varies depending on the industry of the company and/or the category of the data) has the power to collect reports, to make advices and recommendations, and to issue administrative orders to violators regarding their incompliance with the Japanese Act on the Protection of Personal Information (the “Act”).

### Civil Remedies
The Act does not provide specific civil remedies, but violations of the Act may be subject to civil claims for monetary and/or mental suffering damages, and also apology ads as part of tortious claims under the Japanese Civil Code.

### Criminal Remedies
Violations of specific administrative orders issued under the Act may be subject to imprisonment not exceeding six months or a fine not exceeding 300,000 YEN.

### Other Remedies
'Social’ remedies relating to reputation and other relevant business risks may be available, in addition to administrative, civil and criminal remedies.

### Selected Enforcement Actions/ General Comments
Details of administrative remedies (vary on case-by-case basis) may include improvements and suspensions of all or part of violated business activities for compliance with the Act. The amount of damages awarded in civil claims also varies depending on the specifics of the case, and the claims are sometimes made not only on the grounds of privacy invasions but also on other infringements of legal rights/interests such as defamation, unfair trade practices, embezzlement, etc. concurrently.

As general notes, in Japan, an outline of amendments to the Act for utilizing personal data as discussion results of the special committee of the government was publicized in June 2014. And then, a Bill for amendments to the Act has been submitted to the current, annual Diet session and just passed at the Lower House of the National Diet in May 2015. The Bill newly introduces a unified, independent data protection authority, the Personal Information Protection Committee (PIPC) which will be given certain authorities centralizing the personal information protection matters currently administrated by each of the competent ministries in relevant sectors respectively, and also certain personal data activities may trigger filing requirements with the PIPC. However, shortly after passing the Bill at the Lower House, a massive pension data leakage incident was occurred, and as the results of such incident, it is postponed to discuss the Bill at the Upper House, and it is still not certain if or when the discussion of the Bill would be re-commenced at the Upper House in order to make the amendments to the Act effective.
Malaysia

Administrative Remedies

The Personal Data Protection Commissioner ("PDPC") administers and enforces the Malaysian Personal Data Protection Act ("PDPA").

The PDPC has the power to monitor and supervise compliance with the PDPA, including:

(a) implement and enforce personal data protection laws including the formulation of operational policies and procedures;

(b) Conduct investigations where complaints are made to the PDPC or where the PDPC has reasonable grounds to believe there is contravention of the PDPA; and

(c) Issue circulars, enforcement notices or any other instruments to any person.

The PDPC may, in the enforcement notice, direct: (i) data users to take the necessary steps to remedy the contravention; and (ii) where necessary, the data user to cease processing personal data, pending the remedy of the contravention by the data user.

The PDPC does not however have the power to order compensation for damages.

Any person who is aggrieved by the decisions of the PDPC may appeal to the Appeal Tribunal by filing a notice of appeal.

Civil Remedies

There is no express statutory right to pursue a civil claim for non-compliance of the PDPA.

Criminal Remedies

The penalty for breaching the personal data protection principles set out under the PDPA is the imposition of a fine not exceeding RM 300,000 (USD 1 = RM 3.80) and/or imprisonment not exceeding 2 years.

Notwithstanding this penalty, the PDPA also provides for other more stringent penalties in respect of other offences, among others, listed below:

(a) A fine not exceeding RM 200,000 and/or imprisonment not exceeding 2 years for failure to comply with an enforcement notice or failure to process sensitive personal data in accordance with the PDPA;

(b) A fine not exceeding RM 500,000 and/or imprisonment not exceeding 3 years where a person who belongs to a specified class of data user, processes personal data without a certificate of registration;

(c) A fine not exceeding RM100,000 and/or imprisonment not exceeding 1 year where a data user fails to comply with provisions of the codes of practice (which have legal force);

(d) A fine not exceeding RM500,000 and/or imprisonment for a term not exceeding three years where a data user
continues to process personal data after the data user’s registration has been revoked;

(e) A fine not exceeding RM200,000 and/or imprisonment for a term not exceeding two years where a person fails to surrender the certificate of registration to the PDPC when required to in accordance with the PDPA;

(f) A fine not exceeding RM100,000 and/or imprisonment for a term not exceeding one year where a data user continues processing personal data after a data subject has withdrawn his consent by notice in writing to the processing of his personal data;

(g) A fine not exceeding RM200,000 and/or imprisonment for a term not exceeding two years where a data user fails to comply with the requirement of the PDPC to cease processing the personal data of the data subject in a manner that is causing or is likely to cause substantial damage or distress to the data subject or another person;

(h) A fine not exceeding RM200,000 and/or imprisonment for a term not exceeding two years where a data user fails to comply with the requirement of the PDPC to cease the processing of personal data for the purposes of direct marketing;

(i) A fine not exceeding RM200,000 and/or imprisonment for a term not exceeding two years where a data user fails to comply with the directions stipulated in the enforcement notice issued by the PDPC;

(j) A fine not exceeding RM300,000 and/or imprisonment for a term not exceeding two years where a data user transfers personal data outside Malaysia, except to approved places which may be published in the Gazette; and

(k) A fine not exceeding RM500,000 and/or imprisonment for a term not exceeding three years where a person knowingly or recklessly collects or discloses personal data held by the data user or procures the disclosure to another person of personal data held by the data user without the consent of the data user.

Directors, chief executive officers, chief operating officers, managers or other similar officers have joint and several liability for non-compliance by the body corporate, subject to due diligence/ knowledge defenses.(Section 133(a)). There are also regulations issued which supplement the provisions of the PDPA and specific penalties for a breach of the various regulations which we have not summarized.

Other Remedies

Prosecution for an offence can only be instituted with the written consent of the Public Prosecutor. The Sessions Court has the jurisdiction to try offences under the PDPA.

Selected Enforcement Actions/ General Comments

The PDPA came into force on November 15, 2013.

Regulations and statutory orders have also been published and continue to be amended from time to time.
### Philippines

<table>
<thead>
<tr>
<th>Administrative Remedies</th>
<th>None (please see general comments).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Civil Remedies</td>
<td>As specifically provided for by the Data Privacy Act of 2012, individuals or “any aggrieved party” may file civil actions for restitution in court based on the general provisions of the Civil Code (in particular, parties may invoke “abuse of rights” provisions, meddling in privacy and/or quasi-delicts provisions).</td>
</tr>
<tr>
<td>Criminal Remedies</td>
<td>The Data Privacy Act provides for criminal sanctions for violations of its provisions composed of fines ranging from PhP100,000 to PhP5,000,000 (about USD$2,400 to USD$123,450) and/or imprisonment ranging from 6 months up to 7 years.</td>
</tr>
<tr>
<td>Other Remedies</td>
<td>If the offender is a corporation, partnership or any juridical person, the penalty shall be imposed upon the responsible officers, as the case may be, who participated in, or by their gross negligence, allowed the commission of the crime.</td>
</tr>
<tr>
<td></td>
<td>If the offender is a juridical person, the court may suspend or revoke any of its rights under the Data Privacy Act.</td>
</tr>
<tr>
<td></td>
<td>If the offender is an alien, he or she shall, in addition to the criminal and civil penalties prescribed, be deported without further proceedings after serving the penalties prescribed.</td>
</tr>
<tr>
<td></td>
<td>If the offender is a public official or employee and he or she is found guilty of (i) accessing personal information and sensitive personal information due to negligence and/or (ii) processing personal information and sensitive personal information for unauthorized purposes, he or she shall, in addition to the penalties prescribed, suffer perpetual or temporary absolute disqualification from office.</td>
</tr>
<tr>
<td>Selected Enforcement Actions/ General Comments</td>
<td>There are currently no published guidance issued or enforcement actions taken for the provisions of the Data Privacy Act.</td>
</tr>
<tr>
<td></td>
<td>As of this date, the governmental authority or regulator mandated by the Act to be created - The Data Privacy Commission - has not yet been formed. Neither have the Rules and Regulations of the Act been promulgated, even though the Act itself requires the promulgation of the Rules within ninety (90) day of the Act’s effectivity (September 2012) - meaning the rules should have been promulgated as early as January 2013.</td>
</tr>
<tr>
<td></td>
<td>We expect the Data Privacy Commission to be convened and the Rules and Regulations governing the Act to be issued soon as these are long overdue.</td>
</tr>
</tbody>
</table>
Administrative Remedies

The Personal Data Protection Commission (PDPC) has the power to give such directions as it deems fit to ensure compliance, including directions to stop organizations from collecting, using or disclosing personal data or to destroy personal data collected in contravention of the Personal Data Protection Act (PDPA), destroy personal data collected in contravention of the PDPA, provide access to correct the personal data. The PDPC can also direct infringing organizations to pay a financial penalty of up to S$1 mil.

The PDPC currently takes a complaints-based approach towards enforcement, and organizations are not required to proactively register with or seek approval from the PDPC in relation to their activities. Having said that, the PDPC is statutorily empowered to conduct investigations on its own accord to determine whether an organisation is complying with the PDPA.

Directions issued by the PDPC are subject to applications for reconsideration and appeals.

Civil Remedies

Directions from the PDPC may be registered with and enforced by a District Court in Singapore.

The PDPA also provides aggrieved individuals with the right of private action, allowing them to commence civil proceedings in respect of loss or damage suffered.

Criminal Remedies

Contravention of the data protection requirements in the PDPA will generally not amount to a criminal offence. However, the PDPA does provide for criminal penalties in respect of certain “obstruction-type” offences e.g. disposal of personal data to avoid access or correction requests, obstructing or impeding the PDPC in the performance of its duties or making a false statement to mislead the PDPC. Organizations or persons convicted of such offences are liable to fines ranging from S$5,000 to S$100,000 (depending on the offence and whether the offence is committed by an individual or organization).

A failure to comply with obligations prescribed under the PDPA in relation to the Do-Not-Call (DNC) Registry constitutes a criminal offence. For example, a contravention of the requirement to check the DNC registry is punishable with a fine not exceeding S$10,000 (compoundable for a sum not exceeding S$1,000).

Other Remedies

Not applicable.

Selected Enforcement Actions/ General Comments

There have been a few enforcement decisions in relation to violation of the DNC provisions at this point of time, one involving a real estate agent and the other by a tuition agency.
South Korea

**Administrative Remedies**

The Ministry of Security and Public Administration (the “MSPA”) has the power to enforce the Personal Information Protection Law (the “PIPL”).

If the MSPA finds clear basis to support a finding of infringement of personal data and also finds that any non-action in regards to such circumstance may result in damages that may be irrecoverable, the MSPA may order the infringing party to:

I. Cease and desist from engaging in the infringing activity;

II. Suspend any processing of personal data; and/or

III. Take other actions to protect the personal data and to prevent infringement.

Furthermore, if the MSPA finds clear basis to support a finding of criminal activity by a personal data processor resulting from its violation of the PIPL and other laws and regulations on personal data protection, the MSPA may file a criminal complaint with the law enforcement authorities.

In addition, the Ministry of Science, ICT and Future Planning (the “MSIFP”) and the Korea Communications Commission (the “KCC”) have the authority to enforce the Law on Promotion of Information and Communications Network Utilization and Information Protection (the “Information Protection Law”). The MSIFP and/or the KCC may (a) issue a document submission order to any person in violation of the Information Protection Law; (b) issue a correction order to such person; or (c) impose an administrative fine on such person.

Furthermore, the KCC may file a criminal complaint with the law enforcement authorities for any violation of the Information Protection Law.

**Civil Remedies**

Under the PIPL, a data subject that incurs damages due to a violation of the PIPL by a data processor may file a claim against the data processor. In this regard, the data processor may not be exempt from liability unless the data processor shows that it did not engage in intentional misconduct or was not negligent. However, if the data processor shows that it complied with the statutory requirements and was not idle in its duty to exercise due care and control, the liability of the data processor for any loss, theft, unauthorized release, alteration or damages to personal data may be reduced.

Under the Information Protection Law, a consumer that incurs damages due to a violation of the Information Protection Law by a service provider may file a claim against the service provider. In this regard, the service provider may not be exempt from liability unless the service provider shows that it did not engage in intentional misconduct or was not negligent.
Criminal Remedies

The PIPL provides different criminal penalties for different types of activities as follows.

1. **Imprisonment up to 5 years or fine of up to KRW 50 million for:**
   - Transfer of personal data to a third party without the consent of the relevant data subject (including any original collector of personal data).
   - Use or transfer to a third party of personal data without the consent of the relevant data subject.
   - Processing of sensitive data without separate consent.

1. **Imprisonment up to 3 years or fine of up to KRW 30 million for:**
   - Operating a video imaging equipment for the purpose other than the original purpose of installing the video imaging equipment or aiming the video imaging equipment at another location for such other purpose.
   - Acquiring personal data through deception or other improper means or method.

1. **Imprisonment up to 2 years or fine of up to KRW 20 million:**
   - If the personal data in a data processor’s possession is lost, stolen, released without authorization, altered or damaged due to the data processor’s non-compliance with the security requirements.

In this regard, if any officer or employee of a legal entity is subject to the foregoing penalties and the legal entity fails to show that it was not idle in its duty to exercise due care and control to prevent the relevant violations, the legal entity may be subject to a monetary fine.

The Information Protection Law provides for similar penalties.

Other Remedies

PIPL

For lesser violations, such as collecting personal data without the consent of data subject or legal guardian, the MSPA may impose an administrative fine of up to KRW 10 million, KRW 30 million or KRW 50 million for each violation.

Information Protection Law

The MSIFP and/or the KCC may impose an administrative fine on persons who violate the Information Protection Law. In addition, any dispute in connection with personal data may be referred to the Personal Data Dispute Mediation Commission.

Infringement of privacy through the use of information and communications network may be referred to the Defamation Mediation Division.
Selected Enforcement Actions/ General Comments

The Korean law enforcement authorities have been more aggressive in their enforcement of the Korean personal data protection laws since the incident from 2014 that involved a large-scale unauthorized disclosure of customer data from credit card companies (in this case, the employee at a credit information company that released the relevant customer data without authorization was sentenced to 3 years in prison). Following the incident, the Korean law enforcement authorities have formed special joint task force teams for investigation of unauthorized disclosure of personal data. Due to this step, there have been many instances of criminal investigation, and the following is a list of some of the more well-known cases.

- Homeplus, a large Korean distribution company, sold the personal information of its customers collected through a raffle event to an insurance company. Homeplus, including its highest-level management, is under investigation by the public prosecutor’s office.
- An employee at a supplier for Samsung Electro-Mechanics has been arrested for stealing the personal information of the former and current officers and employees of Samsung Electro-Mechanics.
- A Korean pharmaceutical software company is under investigation by the public prosecutor’s office for attempting to sell stolen patient medical records (about 700 million items) to a pharmaceutical consulting company (the president of this pharmaceutical software company has been arrested).
- SK Telecom, the largest telecommunications company in Korea, has been indicted (together with some of its employees) for using the personal information of 150,000 of its customers without authorization.
Taiwan

Administrative Remedies

The Data Protection Authority has the power to investigate complaints and cases, and to order the entity to present relevant information with regard to matters or to take other necessary measures in accordance with the Personal Data Protection Law ("PDPL"). In the event that an investigation reveals that the relevant information is in violation of the PDPL, the information may be confiscated.

Imposition of administrative fines can be up to NTD 500,000 (approx. $15,873) per violation and can be imposed repeatedly until corrective measures are taken; these orders can be appealed to the administrative court.

In addition, the authority has the power to order the suspension of collecting, processing and/or transfer of data, as well as the destruction of data and even publicize the name of the responsible person or entity; these orders can be appealed to the administrative courts.

Civil Remedies

Individuals can seek judicial remedies and damages for breach of the PDPL in accordance with the PDPL as well as the Civil Code.

Class action can also be taken against the violating non-public institution.

Criminal Remedies

Fines of up to NTD 1,000,000 ($31,746), detention and imprisonment of up to 5 years.

Other Remedies

The responsible person within the violating non-public institution will also be subject to same administrative fines as the violating non-public institution unless he/she can prove that he/she performed his/her duties to prevent the violation.

Selected Enforcement Actions/ General Comments

Some examples of recent enforcement actions in Taiwan:

Right to be Forgotten:

In October 2014, a court judgment was rendered awarding a consumer civil damages in the amount of NT$26,000 (approximately US$850) in accordance with the Taiwan Civil Code and the PDPL recognizing a customer's "right to be forgotten."

The case involved one of Taiwan's largest retailers of home improvement and construction products and services which regularly send out unsolicited advertisement emails to its store members. One of its members requested the store to delete his personal information from its mailing list. The store subsequently agreed to do so, yet it continued to send the complainant over 52 advertisement emails over a duration of 6 months after it had agreed to remove his email address from its mailing list.

The court held that this retailer violated the PDPA (Article 3 of the PDPL empowers an individual to request a store to
delete his/her personal information from its system/database. Article 20(2) of the PDPL also stipulates that when an individual indicates his/her unwillingness to receive any marketing materials, the sending company shall immediately cease using said individual's personal information in conducting its marketing activities) and relevant Civil Code provisions and imposed civil damages of NT$26,000.

However, another case rendered in January 2015 and the court rejected the plaintiff's assertion of "right to be forgotten." Thus, while the "right to be forgotten" can be considered a well known concept in Taiwan, how the courts would enforce this right should be closely followed.

✓ Scope of "personal data":

In October 2014 a case involving M+Messenger (a mobile phone communication application which shows its users' mobile phone carriers without users' knowledge and/or prior consent) was brought to the Taipei District Court. In this case a consumer sued the creator of M+Messenger and its affiliate (the marketing subsidiary) claiming his cell phone carrier is considered his "personal data" (which can be used to identify a national person indirectly) and the creator of M+Messenger and its affiliate (the marketing subsidiary) breached his data privacy through unlawfully using his personal data outside the original scope of collection. Both the Taipei District Court and the appellate court found for the consumer recognizing a person's cell phone carrier is considered his "personal data" and thus is cannot be collected, processed or used without complying with the PDPL requirements. In this case, the court awarded the consumer NT$500 (approximately US$16) thereupon. However, this case may have not been finalized.

✓ General comments:

- More and more Taiwanese consumers have the awareness of data protection and are willing to assert their rights with administrative authorities and/or in courts.
- Most government authorities and non-public institution have adopted or in the process of adopting their own data privacy protection measures to comply with the statutory requirements.
- Ever since the effective of the PDPL (in October 2012), more detailed rulings have been issued to deal with unclear issues, e.g., the Regulations for Co-Marketing Activities Conducted among Subsidiaries under the Same Financial Holding Company specified that the consumers are entitled to "opt-in" for the marketing activities and only the consumers' names and addresses can be shared among the subsidiaries in the absence of the consumers' prior written consent.
About Our Practice

Baker & McKenzie has an experienced and widely-recognized Privacy and Data Protection Practice. We advise domestic and multinational companies on all aspects of privacy and data protection (as well as information management) on a global level. Our longstanding dedicated privacy practice is widely recognized as a market leader. We have a keen understanding of the interplay of privacy requirements with labor and employment laws, consumer protection laws, and other local laws. Our understanding of business and operational realities, as well as other practical limitations, enables us to provide balanced and effective advice to guide clients through global information management issues.

Baker & McKenzie assists clients with a vast array of privacy compliance issues, from core compliance steps for the processing of customer and employee personal data to more complex issues such as system and employee monitoring, cross border transfer vehicles, security breach notification and response (see below), hotline implementation, addressing privacy issues that arise in the context of internal investigations and transactions, responding to data access requests and conducting multi-jurisdictional surveys. We routinely advise clients on implementing organization wide privacy programs and help clients track progress via privacy maturity models and other measurement tools.

With regard to breach response, Baker & McKenzie advises clients through the various stages of a security breach. We also assist clients in preparation for possible breaches (including information security reviews, incident response and breach notification policies and scenarios and training). When a crisis does arise, we can provide around the clock litigation support and advice on timing and sequencing of notifications and assistance preparing notifications. We also provide post notification support, including class action litigation and data protection authority and government agency defense.

We provide a holistic approach to managing business information by implementing processes, roles, controls and metrics that treat information as a valuable resource.
Global Data Privacy & Security Leadership Team
This document does not contain legal advice. It may qualify as “Attorney Advertising” requiring notice in some jurisdictions. Prior results do not guarantee a similar outcome.

About Baker & McKenzie

Founded in 1949, Baker & McKenzie advises many of the world’s most dynamic and successful business organizations through more than 11,000 people in 77 offices in 47 countries. The Firm is known for its global perspective, deep understanding of the local language and culture of business, uncompromising commitment to excellence, and world-class fluency in its client service.