Hands-On Guide to GDPR Compliance

Privacy by Design, Privacy by Default

Karen Lawrence Öqvist
Filip Johnssén
Contents

Foreword

Who Should Read This Book?

Introduction
The GDPR Party .............................................. xvii
The DPO Shortage .......................................... xviii
Pick the Low-Hanging Fruit ................................ xviii

Chapter 1: Privacy Foundations
What Is Privacy and Why Is It Important? ......................... 1
Fair Information Practice Principles .............................. 2
  Rights of the Individual .................................... 3
  Controls on the Information ................................. 4
  Information Lifecycle .................................... 4
  Management ............................................... 5
The OECD Privacy Framework ................................ 5
  Collection Limitation Principle ............................... 5
  Data Quality Principle ..................................... 6
  Purpose Specification Principle ............................. 6
  Use Limitation Principle .................................. 7
  Security Safeguards Principle ............................... 8
  Openness Principle ...................................... 9
  Individual Participation Principle .......................... 10
  Accountability Principle ................................ 10
Privacy Dilemmas ............................................ 11
  Freedom of Speech Versus Privacy ......................... 12
  Safety and National Security Versus Privacy ............... 12
Gross National Product (GNP) Versus Privacy .......................... 12
How the GDPR Deals With Privacy dilemmas ...................... 13
Channels of Privacy Invasion ............................................. 13
  Information Privacy .................................................. 14
  Bodily Privacy ...................................................... 14
  Territorial Privacy .................................................. 15
Communications Privacy ................................................ 16
Location Privacy ....................................................... 17
What About Cookies? .................................................. 18
Digital Personal Data Properties ....................................... 19
  Digital Persistence .................................................. 19
  Searchability ....................................................... 19
  Replicability ....................................................... 20
Invisible Data, or the “Unknown Unknowns” ......................... 21
Unintended Processing .................................................. 21
Privacy Is Individual-Centric! ......................................... 21
Who Owns Personal Data? .......................................... 21
Learning Activity ....................................................... 23
Chapter 2: The GDPR
  What It Means After May 25, 2018 ................................. 25
  Compromises (or “Derogations”) .................................. 25
    Lawfulness of Processing ....................................... 26
    Special Categories of Personal Data (Sensitive Personal Data) 26
    Human Resources and Employee Data .......................... 27
    Parental Consent .................................................. 28
Privacy vs Data Protection ............................................. 29
GDPR Made Simple ..................................................... 30
  Material and Territorial Scope .................................... 30
  Key GDPR Definitions ............................................. 31
  Articles and Recitals, What Are They? ......................... 32
  GDPR Tools in Your Pocket ................................. 32
Chapter 3: Controller & Processor Liability

Controller or Processor? ................................. 77
  Who Is the Controller? ................................. 77
  Joint Controllership: How Does This Work in Practice? 78
  Who Is the Processor? ................................. 79
  Who Is Liable? ........................................ 80

Supply Management .................................... 81

International Transfer of Personal Data ................. 82
  Adequacy Decision by the Commission ................. 83
  Appropriate Safeguards Are Provided ................. 83
  Derogations ......................................... 83
  U.S. and the Privacy Shield ........................... 84

Personal Data Inventory ................................ 85
  What the GDPR Says ................................ 85
  Scoping Your Data Discovery Project ................. 85
  Is a Special Tool Needed? ............................ 87

Security of Processing Operations ....................... 89
  Going beyond CIA .................................. 89

“Personal Data Breach” Notification ...................... 91
  What Is a Personal Data Breach? ..................... 91
  When to Press the Alarm? ............................ 92
  Communication to the Authorities ..................... 92
  Communication to Data Subject ....................... 93
  Communicating a Breach ............................. 94

What About Cookies and Marketing? ..................... 96

Sanctions ............................................. 98
  Corrective Powers .................................. 99
  Fines ............................................. 99
  Compensation ..................................... 101

Learning Activity ...................................... 102
Bridge the Gap Between the Business, IT and Legal.......................133
The Legal Gap ........................................................................133
The Business, IT and Security Gap ...........................................136
A Privacy Language for All .......................................................137
EU Versus the Rest of the World ............................................141
Openness and Transparency As a Core Value..........................142
The Privacy Notice .................................................................142
The Privacy Policy .................................................................143
Privacy Intelligence ...............................................................145
The Privacy Hub ....................................................................145
Engagement of Privacy Champions .........................................147
Compliance Through Privacy Standards ..................................148
The ISO 29100 Privacy Framework ........................................148
British Standard 10012:2017 (BS 10012:2017) .......................149
Privacy Metrics ......................................................................149
What are Privacy Metrics? .....................................................150
Choosing Metrics .................................................................150
Learning Activity ....................................................................158
Appendices
Appendix A – GDPR Definitions (Article 4) .........................159
Appendix B – More on Consent ...............................................165
  Informed Consent ...............................................................165
  Freely Given Consent ........................................................165
  Unambiguous Consent .......................................................166
  Specific Consent ...............................................................166
  Opt-in Versus Opt-Out .......................................................166
  Withdrawal of Consent ......................................................167
  Explicit Consent ...............................................................167
  Parental Consent .............................................................167
  Consent to Profiling ..........................................................168
Karen Lawrence Öqvist

“Where and how to start?” That was the first question burning on the lips of every CxO¹ of not only those companies based within the EU, but also any company trading with an EU-based company or EU customers, following the 2016 adoption of the General Data Protection Regulation, or GDPR. Next came a cry for help: “What have we done right—or wrong? And someone please help!” In response, the fall of 2017 brought an array of product and service vendors claiming to have the “magic bullet.” But in reality, many were security and risk products/services repackaged as applying to GDPR.

When it comes to legislation that has data protection and privacy at its core, complexity has triumphed over simplicity and laziness has trumped awareness. As a result, there has been a lack of compliance and adoption on the rights of the data subject.

Despite the imperfections that you will hear concerning the GDPR, one thing is for sure: It is better than what we had before. Fundamentally, it attempts to achieve two conflicting goals:

- Facilitate the flow of personal data across national jurisdictions within the EU—after all, Gross National Product (GNP) is important for the growth of us all!

- Protect the privacy of EU data subjects, a goal that stems from the 1953 European Convention on Human Rights.

What strikes me foremost within the legal text of the GDPR, which I really don’t like, are the exemptions when it comes to sharing personal data in the name of “national security” and “law enforcement.”²

¹ A collective reference to C-level corporate executives.

² The exchange of personal data within the context of law enforcement is regulated in the directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention,
Moreover, there is the rather sneaky clause concerning “legitimate interest” (Article 6(f)). We’ll talk more about these issues later in the book!

However, as a whole, the GDPR tries to fix what was broken before, and more. It attempts to update laws that were outdated and not aligned with today’s digital and connected society. It succeeds where other attempts have failed. And in the future, it will fall short, too. After all, technology evolves rapidly, and tried and tested legislation takes much longer to craft and implement. But we must focus on what we have in place and what we know today, not on the unknowns.

Up until recently, issues pertaining to compliance with national data protection laws have been addressed by legal consulting companies or the legal arm of an organization. Yet the Internet of Things (IoT) is the Joker in the pack of cards for the legal profession. IoT is collecting heaps of personal data on each of us. The GDPR is a response to the IoT; to the technology that tracks our choices and our movements, both in the physical and digital worlds, which are now overlapping, the boundaries impossible to separate. We have, each of us, become enmeshed in a digital society.

The GDPR is a new breed of animal graced with a rather impressive set of teeth. Should a data controller show that they are not fit custodians of personal data by losing or otherwise exposing such data, the entity can be fined up to four percent of its annual revenue for each data loss—in addition to the potential damages that can be awarded to the data subject. In other words, this rather “hot potato” has landed at the board level of any international or company operating within the EU. This is not just controllers, it is also the processor who doesn’t want to be held liable for the mistakes of the controller. They need to limit the scope of accountability. In many cases, this “hot potato” is too hot for the board, and in turn has been delegated to either the CIO or the compliance arm of the organization. On the surface, this might seem to be a good thing, except many experts are unaware that compliance with the GDPR is not the same as compliance with investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data.
Sarbanes-Oxley³, Basel III⁴, PCI-DSS⁵, or any infosec program using ISO 27002 as its control framework. GDPR compliance is not a tick-box exercise!

Confusion has come about because these programs, namely the ISO 27002 control framework, has a specific section on compliance with data protection laws. This has resulted in infosec professionals attempting to map privacy compliance into security compliance. That’s the wrong approach. And that’s why I wrote this book: to explain in a simple way how to deal with compliance with the GDPR.

I am not a legal guy, I am an information security guy (or girl, as the case may be). I have over the years become a geek in IT, digital identity, information security, compliance, privacy, business, management change, and entrepreneurship. I believe that to get this right, we need to do better than we have in the past with information security, which was in all honesty a journey of compromises.

I have been partially inspired by David Lacey, the founder of the Jericho Forum and the brains behind BS7799, which later evolved into ISO 27001. He had and still has a capability to find simplicity within complexity. He has provided me with inspiration to strive for the same level of simplicity in everything I do.

I found additional inspiration in the work of Fred Piper, founder director of the Information Security Group (ISG), and professor at the Royal Holloway University of London (RHUL). He is so highly respected and he explains complicated subjects in such a simple way you wonder really if they really are so complex.

Also influential was a book⁶ by Margaret Wheatley, who linked management practices with physics and nature and showed how order and structure underlay the chaos and complexity of the natural world—a lesson that can be applied to organizational thinking.

Finally, there is the International Association of Privacy Professionals (IAPP). It was during my first IAPP Global Privacy Summit in Washington, D.C., in 2015 that I heard the keynote Glenn Greenwald talking about whistleblower Edward Snowden and the responsibility of digital privacy officers in the modern age. It was

---

³ See http://www.soxlaw.com/
⁴ See https://www.bis.org/bcbs/basel3.htm
⁵ See http://www.theukcardsassociation.org.uk/security/What_is_PCI%20DSS.asp
⁶ Leadership and the New Science: Discovering Order in a Chaotic World
immensely inspiring. Following this I became certified in CIPP/E, CIPT, and CIPM. I also discovered the Organization for Economic Co-operation and Development privacy principles, which I consider to be the lowest common denominator in privacy globally.

These four influences have driven my thinking for at least the last 10 years, and also how I have approached writing this book. A final inspiration was Filip Johnssén, who agreed to co-author this book with me. He is a legal geek, philosopher, and comedian, and someone who I am privileged to have as my sounding board and friend over the last two years.

Filip Johnssén

With the release of this book I celebrate a decade of working exclusively with data protection, or as I prefer to call it, “data privacy.” To me “data protection” sounds almost like “information security.” Not that there’s anything wrong with information security, but that term tends to diminish what the field is all about. The origin of data protection can be found in the field of human rights, not IT. It’s about the protection of each of us in our capacity as living human beings. We all have an inherent right to privacy. The size and limits of the private sphere are perhaps still open for discussion, but almost everyone agrees it exists to a larger or smaller extent.

A subset of privacy is data privacy. As the digitized world continues to grow and evolve, this realm gets increasingly important. As we are still at the beginning of this trajectory, it is hard to forecast how data privacy will evolve in a few decades. But what we do know is what the legal framework in the EU looks like from May 25, 2018—it looks like the GDPR. And as with all data protection legislation, it is thereafter all about the implementation. And that is what we have in focus in this book. As far as possible we have tried to exclude complicated legal lingo or deep dives into legal subtlety.

However, I will here and now discuss some of the more philosophical aspects of GDPR. First of all, I can’t get away from the feeling that most debaters seem to think the GDPR is something new that just fell down from the sky, or that we started arguing these issues in 2012. Nothing could be more wrong. The concept of privacy has been around as long as mankind; one can find mention in written texts dating back to Aristotle
(4th-century BC), Risalat al-Huquq\(^7\) (Second half of 600), the Magna Carta (1215), and later the European Convention on Human Rights\(^8\) (1953).

Meanwhile, an interesting conundrum is that when privacy is explicitly mentioned it is never defined. Quite often I ask myself if it’s even possible to agree on a definition. My conclusion stays the same: No, it’s not. It is through this lens that I understand privacy laws and their implications as well as why they look as they do. The GDPR is not an exception. The ultimate question, then, becomes: Is it possible to legislate about privacy? Were the politicians in Brussels correct to adopt a regulation applicable throughout EU? To me this is still an open question and only time will tell.

Don’t misunderstand me. I do like the idea of having one general data protection legislation cover the whole of the EU, but I don’t know if it will work. Privacy is not a cucumber. We all remember the debate that followed the EU stating how a cucumber should look.\(^9\) Now the EU has tried to state how big the privacy sphere is. But unlike a cucumber, privacy is not measured in centimeters or kilograms. It is an individual experience. What is OK in one situation is not OK in another. Yes, private life needs to be safeguarded, no question about it. But should it be safeguarded in the same way regardless of the contextual, social or historical background? In some sense this goes back to the ongoing debate about legal positivism\(^10\) versus natural law.\(^11\) Even though this is germane to discussions about the GDPR, this political science is not what we will focus on in this book.

For now, let’s just accept the GDPR as it is, pros and cons, and try our best to implement it in an easy way. In this book I, together with my very good friend Karen Lawrence Öqvist, will share anecdotes and tips for implementing legal data privacy requirements in a smooth and

---

7 Treaties on Rights.
8 The European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR).
10 Legal Positivism is the notion that the law reflects the society and the social order as well as the structure of governance. The law is not measured on its own merits, but its role in society.
11 Natural law is the belief that there are some rights common to all humans in their capacity as humans and that these are not derived from the society and its norms.
effective way. I am very fortunate to have Karen as a friend and co-writer. Whenever I have lost myself in philosophic reasoning, she has pulled me back on track.

I should also state I don’t share Karen’s view that surveillance is necessarily something bad. Maybe my five years in the Swedish Security Service indoctrinated me to think otherwise. Cameras and wiretapping are not the devil’s tools. They are in the public interest.
Who Should Read This Book?

This book takes GDPR compliance straight from the field. It is an operational book, although we delve into big-picture privacy and GDPR questions and topics in order to migrate you into a “privacy” and “legal” mindset. We have tried to keep the “legal speak” to a minimum, but frankly there is no way you will get into a seasoned role as a GDPR practitioner without some exposure to the legal thinking behind the text.

If you are an IT, security, and/or compliance practitioner who has been tasked with GDPR compliance, then this book is definitely for you. It will extend your skillset into privacy and GDPR.

This book is not a comprehensive GDPR legal guide. If you are a legal professional, this book will broaden your knowledge about how to take a legal instrument and convert into an implementation tool. But if you are looking for a pure GDPR legal focus, this book is not for you.
The GDPR party

After a slow start, things accelerated during 2017, organizations woke up from their coma, and most had a budget to roll out their GDPR projects. (Those that didn’t are in a state of panic!)

A common mistake is for organizations to use the GDPR per se as the toolbox to implement compliance across their organization. Earlier we mentioned that the GDPR is a piece of legal art. Hence, it is not a toolbox. It does not explain how to implement. It states you need to have data protection by design as the default mode of operations across your business, but it does not say precisely how to achieve that goal.

We heard over and over that one cannot take a “tick-box approach” to GDPR compliance. So here we have a legal piece of art, that is not styled to execution. Those who have tried have ended up in a GDPR quicksand, saddled with a humongous project, sucking up resources with no end in sight. The legal team is quoting the GDPR principles, while the IT and security guys still think you can treat personal data the same as intellectual property (IP). Regardless, both camps appear to neither understand the basics nor to have consensus on how to approach GDPR.

GDPR product vendors are claiming they can make your organization GDPR compliant, simply with a magic bullet. Unfortunately, many of these “snake oil” offerings are merely security products repackaged as privacy products. The IT and compliance team are easy targets because they may not understand the complexity of the GDPR as well as the data protection legal team does. After a trillion breakfast seminars—mainly sponsored by companies wanting to sell them products and services—the IT, security, and compliance guys are like the blind leading the blind. In short, “snake oil” is a hot commodity on the GDPR market in 2017 and that is likely to be the case until at least 2020!

Often, the legal team understands the complexity, but doesn’t know how to implement across the business. There are exceptions, and that is where the legal department happens to support a business wherein personal data is the core product, like in the insurance sector. However, the majority of legal professionals have problems communicating with the compliance/IT guys. If GDPR compliance is run by IT there is a trend to conduct privacy risk assessments on IT systems.

Then there’s the business executives, who are standing back, expecting this to sort itself out before they get called in to the party. This is a big problem because in order to get data protection by design as a default you need to start with the business functions, and see that you have documented the business processes and assigned ownership. Getting everyone on the same page is the foundation to effectively assessing privacy risk across your organization along with getting an GDPR accountability structure in place.

The DPO shortage

In 2017 the market for the Data Protection Officer (DPO) role in the organization is forecast at circa €6 billion following May 25, 2018. This position is a requirement for many large organizations, especially those which deal with sensitive data, and particularly if that is the core product of a business. Even if an organization does not have, or need, someone in this role full-time, companies will have to incorporate this expertise somehow on their GDPR journey to compliance.

Pick the low-hanging fruit

Many organizations have started on their GDPR journey, and risks are surfacing to expose gaps that point to opportunities to do what should have been done previously.

But you don’t need GDPR experts to do all your work. They are after all in short supply and there are a lot out there selling “snake oil.” You can get the ITIL/ITSM experts in to fix your IT processes; for business processes, get the black belt in Six Sigma; and for security the infosec guys. Follow industry standards, get the rules in place, document, evidence and find yourself in a nice place when you can focus on personal data.
Privacy Foundations

CHAPTER 1

Privacy Foundations

What is privacy and why is it important?
Privacy per se first hit the press big time in 1890 when a paper, “The Right to Privacy,” was published by the Harvard Law Review. It turned out to be “one of the most influential essays in the history of American law”¹ and is widely regarded as the first publication in the United States to advocate a right to privacy. It interprets that right primarily as a “right to be left alone.” The paper was written by Louis Brandeis and Samuel Warren. Brandeis was an American lawyer and associate justice on the Supreme Court of the United States from 1916 to 1939, and he later acknowledged that the idea for the essay came from Warren’s “deep-seated abhorrence of the invasions of social privacy.”²

Article 12 Universal Declaration of Human Rights
No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

Since 1890, the base assumption of the right to personal privacy has been recognized around the world in diverse regions and cultures. The Universal Declaration of Human Rights,\(^3\) adopted by the United Nations General Assembly in 1948, includes a right to privacy in Article 12. This was adopted by the European Convention on Human Rights (ECHR) in 1953. Nearly every country in the world includes a right to privacy in its constitution, and if it is not defined explicitly, it is generally acknowledged implicitly as a right.

Privacy is an inherent concept for humanity, yet it presents many dilemmas in society. A particular conundrum is that ideally, we each want privacy for ourselves, yet we would like everyone else to be transparent. This makes absolute privacy per se a difficult feat for any society.

‘Whenever a conflict arises between privacy and accountability, people demand the former for themselves and the latter for everyone else.’

—David Brin, The Transparent Society, 1998

This dilemma and more are tackled in the form of privacy laws, which are created to protect us from potential invasions of individual privacy, including either deliberately or accidentally by those collecting and processing personal data.

The initial building blocks behind today’s privacy laws came in the form of privacy principles, such as those created by the United States with the Fair Information Practice Principles (FIPPs) in 1973.

**Fair Information Practice Principles**

It was in 1973 that the U.S. Department of Health, Education and Welfare codified the FIPPs\(^4\), which provided best practices on the handling of personal data—referred to as personally identifiable information (PII)\(^5\). FIPPs were a first attempt to take something complex

---


5 Any information that permits the identity of an individual to be directly or indirectly inferred, including any other information which is linked or linkable to that
and simplify it into actionable bullet-points. We provide this overview because privacy principles, laws and regulations devised globally thereafter were greatly influenced by FIPPs.

Within FIPPs, four principles on privacy are defined:

1. Rights of the Individual
2. Controls on the Information
3. Information Lifecycle
4. Management

**Rights of the Individual**

This principle states that organizations must provide notice about their privacy policies and how personal data is used. Choices should be presented to individuals on the collection, use, retention and sharing of personal data. It is here the concept of “opt in” and “opt out” consent was first presented to individuals.

![Figure 1. FIPPs Rights of the Individual](image)

Individual regardless of whether the individual is a U.S. citizen, lawful permanent resident, visitor to the U.S., or employee or contractor to the Department.
Controls on the Information

This refers to the protection of personal data with information security controls, and the responsibility of the organization to ensure that personal data is kept up to date, i.e. data quality is preserved.

Information Lifecycle

This starts with data **collection**, and states that organizations that collect personal data should collect only what is needed for the purpose identified in the privacy notice. Organizations should only **use** personal data for the purposes described in the privacy notice; **retain** it for only as long as the purpose requires; and finally, **disclose** to third parties nothing outside of what is communicated within the privacy notice.
Management

The management principle covers what needs to be done to ensure the other three principles are implemented. This is to do with assigned **accountability** for the creation and application of privacy policies and procedures, along with **monitoring** and **enforcement** mechanisms to ensure that the organization is following what is written and communicated in privacy policies and procedures.

![Figure 4: FIPPs Management](image)

The OECD Privacy Framework

In 1980, the Organization for Economic Co-operation and Development Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (OECD Privacy Framework) guidelines were created, providing further foundations for privacy practices and regulations. These principles have become the basic building blocks of privacy laws in every country worldwide. For obvious cultural reasons, there are slight differences both in content and denomination, but from a theoretical perspective, they are the same. (Argentina and Mexico are just two countries with privacy laws containing principles very similar to those outlined in the OECD Privacy Framework.) These principles could effectively be considered the lowest common denominator in privacy globally.

Collection Limitation Principle

*There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.*

Collect only what data is needed for the specified purpose, and if needed, get consent. For example, if your organization uses a web form to capture personal data in order to deliver a book ordered by a customer, the form...
should only include fields that are absolutely needed for the delivery of
the book, nothing more. You could include a dropdown list of choices
instead of a free-text box to restrict what the user is able to share. The
collection must be strictly aligned to the specific purpose for collection,
which is quite simply the delivery of the book.

Even at this stage, the need for openness and consent of the individual
(i.e. data subject) is at the forefront. You will recognize distinct
similarities with the first step (Collection) in the FIPPs Information
Lifecycle privacy principle.

Data Quality Principle

*Personal data should be relevant to the purposes for which they are to be
used, and, to the extent necessary for those purposes, should be accurate,
complete and kept up-to-date.*

If you are a security professional, you would be forgiven in mistaking
this for integrity, as in the “Confidentiality, Integrity and Availability”
(CIA) security triad which has provided the grounding rules on securing
data for ages—even before the BS 7799 control framework became the
adopted industry standard within information security (today known as
ISO 27002, part of the ISO 27000 family).

What this principle is really about is in fact the quality of the data
pertaining to the individual. This is personal data that changes during
our lifetime. We move, we change names, we change our habits, and our
health fluctuates. Our personal data must be kept up-to-date, and this is
the responsibility of the organization or public entity that has collected the
personal data. You can see that this principle is derived from the FIPPs
“controls on the information” privacy principle, i.e., information quality.

Purpose Specification Principle

*The purposes for which personal data are collected should be specified
not later than at the time of data collection and the subsequent
use limited to the fulfilment of those purposes or such others as not
incompatible with those purposes, and as are specified on each occasion
of change of purpose.*
There must be a specific purpose for the collection of personal data. If there is no purpose you should not be collecting it. It is that simple! Although, in practice, it is not.

Take the example that you buy a book on booksonline.com. The reason why you share your name and address is to deliver the book to your home. You may also share your credit card details, to pay for the book.

The purpose could purely be “client buys book,” which combines both the “delivery of book” and “payment for book” into a single purpose. However, it would be more specific to create a separate purpose for each; the risks and collection channels over which personal data will travel over are distinctly different, and these implications become obvious when conducting a privacy impact assessment (PIA).

What is more, the purpose of personal data collection should be communicated to the data subject at the time of collection, whether through an external-facing privacy notice, or some other notice.

What is meant by “incompatible”? This means that any use must be compatible with the original stated purpose. See the next principle.

**Use Limitation Principle**

*Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.*

How does your organization use personal data following its collection? The purpose specifies what you are using personal data for, and the use is basically how you do this. For example, an individual orders a book on booksonline.com. The purpose “delivery of book” means that the department responsible for the delivery of the order receives only the personal data needed to get the book to the customer, e.g., name, address, book ordered, and delivery choices. For the related purpose “payment of book,” there will also be a legal obligation to store financial data for 10-15 years, which is a legal requirement, and another use.

Personal data collected for the purpose of providing a harmonious user experience, such as the placing of cookies to store the customer’s buying habits, is not compatible with either of the above purposes.
This data not needed to fulfil the delivery of the book, or to process the financial transaction. It will be used by marketing. In order to follow these rules, it is smart to create a separate purpose for marketing and the use of cookies. Each use must fall within the confines of each specified purpose.

If you take the FIPPs Information Lifecycle, it is easy to see how the Use Limitation Principle is a part of that lifecycle. Use is not only what you do with data, but what you do not do, including storing or sharing personal data, both internally and externally with third parties.

Security Safeguards Principle

*Personal data should be protected by reasonable security safeguards against such risks as: loss or unauthorised access, destruction, use, modification or disclosure.*

If you are an information security professional, you will have realized by now that privacy is much more than information security. Clearly, it is impossible to have privacy without information security; there must be adequate technical, management and organizational measures implemented to protect personal data. After all, information security is about the protection of personal data, and ensuring it is available when needed to minimize service disruptions.
The challenge for information security professionals is that whenever new methods are developed for creating or collecting, storing, or transmitting information, these innovations are almost inevitably followed by methods of harnessing the new technologies and protecting the information they process. Since the 1990s, the confidentiality, integrity, and availability (CIA) model has been the de facto standard by which to design and build an organization's information security architecture.

The domain of information security has been around so long you would think, “it’s not rocket science,” but it is. “So much has changed in the way we store data, where we store it, how we transmit it, and how we secure it. Moreover, ensuring data security and protecting privacy is becoming harder as the information multiplies and is shared ever more widely around the world. The threats to information confidentiality, integrity, and availability have evolved into a vast collection of events, including accidental damage, destruction, theft, unintended or unauthorized modification, or other misuses from human or nonhuman threats,” writes security engineer Georgie Pender-Bey.6

Openness Principle

There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

FIPPs considers openness under Right of Individual. An example of openness is the external-facing privacy notice that informs the data subject of the purpose for the collection of personal data, and what is done with it after use. There could be other legal obligations on reporting to national data protection authorities according to national privacy laws and regulations, such as with health care data, clinical trials, credit card data, etc.

An individual should have the right:

- to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;

- to have communicated to him, data relating to him, within a reasonable time, at a charge, if any, that is not excessive, in a reasonable manner, and in a form that is readily intelligible to him;

- to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.

Individual Participation Principle

The expectation for public notice, data subject access, with choice and consent for the individual also stems from the FIPPs Right of Individual. The OECD principles extend these expectations so that the individual is able to request information about who is collecting their personal data, and what is being done with it. Moreover, the individual should have the right to request that personal data is amended/updated if the data quality principle is at issue, or erased if the use of personal data is not compatible with the purpose for collection.

A data controller should be accountable for complying with measures which give effect to the principles stated above.

Accountability Principle

Basically this means there needs to be evidence of data protection compliance and implementation of measures and policies to meet the requirements laid out in the principles, such as ensuring the rights of the data subject are responded to, etc.
Privacy Dilemmas

Every privacy law presents the challenge of balancing the right to a private life against national safety and commercial growth. Factors such as culture and political structure influence how privacy laws are implemented in those countries that have them.

What’s more, every privacy law globally is challenged by realities of the so-called “Information Age”—a term coined at the beginning of this century that has grown to encompass the “Internet of Things” (IoT), “data analytics” and “Big Data.” This has, over the last 30 years, unleashed a surveillance society: A multi-faceted beast that started its life in the form of cameras overlooking public spaces such as subways and football grounds (referred to as “Big Brother”), and has evolved to include a proliferation of personal data collection devices. Now we have the “Little Sister” phenomena: Sensors, GPS and location services running on mobile phones, smart watches, fitness trackers, and other wearables, and intelligent home systems have all extended the reach of surveillance to sousveillance and life-logging. As a consequence, personal data has become a tangible commodity which can be bought and sold if national privacy laws permit. It is the users of these devices that privacy laws are created to protect.

What is Internet of Things (IoT)?

Wearables, intelligent homes, sensors, Global Positioning Systems (GPS), Location Based Services (LBS), the black box in your car, are all examples of the IoT. Personal data is being collected without the knowledge of the data subject. They are “passive” in the collection. Although the individual may have enabled collection through a wearable, an app on a mobile device, etc., they are not “active” in sharing their personal data. The individual is potentially unaware to the extent of personal data being collected in their environment which is becoming more and more ubiquitous.
Freedom of Speech versus Privacy

Some countries refer to this concept as freedom of speech, others use freedom of information or freedom of expression. For simplicity, we are using the term freedom of speech, but we refer to any such right.

One of the principal challenges of every country that has implemented privacy laws is how that law co-exists with freedom of speech protections. We need both in order for a democratic society to function effectively.

Safety and National Security versus Privacy

Society needs to be protected from illegal activities and potentially dangerous individuals and criminal organizations. This has been an ongoing discussion: How far can you go in the invasion of privacy in the name of law enforcement?

The GDPR has exemptions to the rights of the data subject (Individual Participation and Openness Principles) for law enforcement and national security activities. There are other laws controlling access by government authorities in their role as law enforcement and intelligence gathering agencies to personal data. In Article 6(e) of the GDPR you will find that “national interest” is a legal basis for processing.

Gross National Product (GNP) versus Privacy

It was mainly businesses, government authorities, law enforcement and national security agencies that lobbied for the flow of personal data. In order for society to function there needs to be controlled access by government authorities in their role as law enforcement and intelligence gathering.

On the other side have been privacy advocates, representatives on behalf of the data-subject and the data subjects themselves.

Table 1. Conflicting goals of data protection in the EU

<table>
<thead>
<tr>
<th>Society needs to function</th>
<th>Right to privacy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Permit flow of personal data among member states</td>
<td>Protect the privacy of E.U. data subjects</td>
</tr>
</tbody>
</table>
How the GDPR deals with privacy dilemmas

The GDPR does its best to balance these conflicting dilemmas, starting by placing the individual at the center. Moreover, the legal text of the GDPR has shifted away from the analog world upon which its predecessor directive was based (Data Protection Directive, 1995) and toward the digitized world of today. It also provides a foundation for the future. This makes the GDPR a complex piece of legislation and despite the voice of some critics, it is nonetheless a piece of legal art of which we can, within the EU, be proud. As with any piece of art, it has its purpose. It is written by lawyers for lawyers. As with any law, it will be tested up to the highest courts within the EU during its lifetime. It is a law that sets the rules of play pertaining to data protection within the EU. What we have is a baby with a strong DNA, and we will see case law determine its character during its lifetime.

Channels of privacy invasion

These “privacy types,” representing different channels for invasion or breach, were originally identified by Privacy International more than 10 years ago. While no reference can be found on their website today, the categorizations live on in privacy impact assessment guides offered by places such as Ontario, Canada, and Victoria, Australia (along with an additional type referred to as location privacy).

<table>
<thead>
<tr>
<th>Privacy Type</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information Privacy</td>
<td>Privacy International</td>
</tr>
<tr>
<td>Bodily Privacy</td>
<td>Privacy International</td>
</tr>
<tr>
<td>Territorial Privacy</td>
<td>Privacy International</td>
</tr>
<tr>
<td>Communications Privacy</td>
<td>Privacy International</td>
</tr>
<tr>
<td>Location Privacy</td>
<td>Victoria, Australia PIA</td>
</tr>
</tbody>
</table>

The document created by the Privacy Impact Assessment Framework (PIAF)\(^7\) consortium and prepared for the European Commission

---

Directorate-General for Justice in 2011, which compared privacy impact assessment guidelines internationally, recommends the use of these five privacy types, which consider privacy beyond information privacy.

We will now discuss the privacy types in more detail.

**Information privacy**

Information privacy protects personal information and involves the establishment of rules governing the collection and handling of personal data such as credit information and medical and government records.

Information privacy is the most well understood part of privacy because it was around even before digitization took over our lives; it includes personal data that you share with your employer, health care provider, local government authorities, banks, insurance agents, etc. It is the sensitive data that has been collected on us, traditionally in paper format and migrated into a digital format over the last 20-30 years.

Information privacy in practice is when you fill in a form with personal data. It could be to order a book, or to register for a newsletter. You, as the data subject, are *active* in sharing your personal data, and typically aware of what you are sharing.

**Bodily privacy**

Bodily privacy protects the integrity of the physical person against invasive procedures such as genetic tests, drug testing and cavity searches.

From biometrics to DNA or drug tests to body scans, technology that just 10 years ago was the content of sci-fi films (or limited to the realms of law enforcement) has now infiltrated our daily lives. We use our fingerprint to use our iPhone, send our DNA to be analysed for hereditary diseases, submit to random testing for substance abuse in the workplace, and enter body scanners when we travel at airports.

**Biometrics**

It has become the standard to include biometrics in our passports and ID cards. Biometrics were once considered very intrusive to our privacy, although the use of biometrics is becoming more commonplace nowadays.

A biometric is a physical and unique characteristic of an individual. Examples include your fingerprints, hands, face, irises, gait and behavior. The use of a fingerprint to access your iPhone is an example of biometric authentication as is the use of biometrics (both fingerprint and iris) as a gun safety feature, ensuring the firearm can only be used by the authorised owner and/or user.

Some countries are using facial recognition systems, which match the biometrics on your passport with what is returned by scanning devices, at their borders. If the match is positive you are permitted through.

DNA
Did you know that your DNA is sensitive data? And that each person’s DNA is unique except for identical twins?

Not only does genetic information provide something like a fingerprint through variations in genetic sequences, it also provides a growing amount of information on genetic diseases and predispositions. Errors in the genetic code are responsible for an estimated 3,000-4,000 hereditary diseases.

Territorial privacy
Territorial privacy protects personal space, objects and behavior; consider the setting of limits on intrusion in the domestic sphere and other environments such as the workplace or other public and private spaces. Such intrusions can include searches, video surveillance and ID checks.

Surveillance
George Orwell's book 1984 predicted a Big Brother state as the fate for our society. In reality, our society has evolved into more of a Little Brother/Sister state. Surveillance has become widespread, but is not government dominated; rather, it is disparate and disconnected. Video surveillance through CCTV (closed-circuit TV) is used to monitor public and private spaces worldwide. There are laws in most countries restricting the use of CCTV. The requester must have a solid reason for installing CCTV cameras, and must get approval from the relevant government authorities.
“Sousveillance”

Up until 10 years ago, surveillance was conducted only in the name of public safety and law enforcement, but that was until the smartphone hit the streets and brought us into a new dimension of “sousveillance.”

The term sousveillance is derived from the contrasting French words sur, meaning “above”, and sous, meaning “below.” While “surveillance” suggests an “eye in the sky” watching from above, “sousveillance” denotes bringing the camera down to human level (an individual is watching, rather than government authorities or private industry). The first person to start the trend of sousveillance was Canadian researcher and inventor Steve Mann, who has been dubbed “The Father of Wearable Computing.” He’s been walking around with a camera strapped to his head recording his life since the 1980s. Since that time, wearables have evolved from large and clumsy to the elegant Google Glass that can be purchased today. Furthermore, sousveillance is even what we are doing with our mobile phones, taking photos and video often without the knowledge of the data subject.

ID Checks

An ID card is required in order to conduct an ID check. Your ID card is a legal document providing evidence that you are who you say you are. Some ID cards created by government authorities include biometric data.

ID checks are done to validate your identity by border controls at the airport and to check you are of a legal age upon the purchase of restricted items such as tobacco and alcohol, for example.

Communications privacy

Communications privacy protects against eavesdropping on mail, telephone calls, email and other forms of communication.

Any voice communication that runs over telephone networks is included; this not only includes contents of voice conversations but also something called metadata.

Every time you make a call, information about that call—including who you call and how long you are connected—is stored for a short time by the telecommunications provider as metadata. There are laws implemented in most countries globally requiring operators to store...
metadata for an extended period of time in the name of law enforcement. Many of the international laws on wiretapping date back to a series of seminars hosted by the FBI in 1993 at its research facility in Quantico, Virginia. The seminar was called the *International Law Enforcement Telecommunications Seminar (ILETS)* together with representatives from Canada, Hong Kong, Australia and the EU. The result was an international standard called the *International Requirements for Interception*, which was adopted by the European Union in 1995. This standard sets out a legal requirement for all telecommunication providers and equipment manufacturers to build surveillance capabilities into all telephone systems.

**Location privacy**
Location privacy protects against surveillance via anything “smart” that you wear or use. Such technology is a ubiquitous part of our modern lives: location based services (LBS), Global Positioning Systems (GPS) and Radio Frequency Identifiers (RFID) used by wearables and sensors in your home, workplace and basically everywhere you move around.

In this case, the user is passive in the collection of personal data. This means that once the service is enabled, the user of the service does not need to do anything to facilitate data collection. This is one of the characteristics of the Internet of Things (IoT).

**Global Positioning System (GPS)**
GPS is something we have been using traditionally in our cars to find the right way to our destinations. However, its uses are expanding—tracking taxis or delivery vehicles, for example. This data is stored in a black box, which can be used following an accident. The speed of a car at impact together with GPS data is revealing.

**Location Based Services (LBS)**
With the download of an app on your mobile device, tracking can pinpoint your location at any given moment in time. You can use such services to find a coffee shop in the local vicinity, or the closest airport lounge.
Radio Frequency Identifiers (RFID)
RFID is a technology that is turning virtually every item in our static ecosystem—from your coffee machine to your clothes to the lighting in your house—into a living ecosystem, converting personal habits and activities into a digital format, hence one that can be intelligently analyzed, correlated and mined. RFID tags today are embedded in items, clothes, living animals and individuals. The sensors have uses ranging from helping your car with parking to assisting in search and rescue missions (with the embedding of an RFID chip in ski and mountain wear).

The combined use of GPS and sensors is also leading a revolution in driverless cars, enabling them to be tracked in real time from an offsite control center as well as helping to monitor conditions and control speed, all without any driver input.

What about cookies?
One of the most pervasive privacy invasions not covered here is the use of “cookies.” Cookies are downloaded onto your computer to keep a track of what you are doing when you browse a website. If we were to define the type of privacy that involves cookies, it could be called “device privacy.”

Cookies collect personal data of which you are not aware, you just see the results, e.g. books you have browsed when visiting an online bookstore. They were developed to enhance the user experience, but today their use is abused. Cookies and more will be covered in the GDPR’s ePrivacy Regulation due to replace the ePrivacy Directive. The timeline for that, as of this writing, is unknown. The text has not yet been finalized, but what is certain is that “choice” will be key. To protect device privacy, a user of a web service should not be forced to accept cookies outside of what is absolutely necessary to provide that service.
Digital Personal Data Properties

Digitized data has properties beyond those that were considered before society went digital and online. Irrespective of whether personal data is user-generated or not, four properties apply:

- Digital persistence,
- Replicability,
- Searchability
- Invisible audiences

In the application to personal data we have adapted the concept and appended a fifth property: unintended processing.

Digital persistence

Everything you share online is digitally stored on multiple servers somewhere. Why multiple servers? All data digitally stored is normally “mirrored” in order to meet availability requirements, e.g., if one server becomes unavailable or overloaded with traffic, a mirror site will take over the request from the user. Additionally, all data is stored on backup media somewhere. This data will persist until the media is overwritten, and this should be determined by a security policy on media rotation.

The persistence property is a trigger for the Right to Erasure within the new GDPR. Execution of this right needs to be reasonable. The question of personal data stored on backup tapes is common; this can be dealt with by following the industry standards for information security pertaining to backup and media rotation. For example, every three months, backup tapes are re-used, i.e., overwritten.

Searchability

This takes us to the Right to Be Forgotten (RTBF), as defined in the GDPR. When you are searching for data pertaining to an individual online, the search engine, using its complex analytics and small virtual

---

8 Danah boyd, a well-known researcher and expert on young people and how they use social media, defined that the “mediated public” was referring to user-generated content created in online spaces.

spiders, finds all related data. You can liken this to the index in a book. The Right to Be Forgotten does not remove contents of the book in this example—that’s the Right to Erasure. RTBF removes the specific index which references a specific individual in the book. The Right to Erasure has been around since the EU’s Data Protection Directive of 1995, stating that personal data must be erased if a specific purpose for processing is lacking.

The most publicized driver behind the RTBF can be found in the judgment of Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González (C-131/12). The press was for a time full of articles and opinions about whether RTBF is a practice that inhibits the freedom of expression, or whether individuals should be free to exercise this right.

The European Court of Justice judgement pertains purely to search results and auto-complete functionality within the Google search engine. It is not about the original content. What this ruling is about is search engine results and intelligent auto-complete on searches for personal data, linked to an individual who is an EU data subject, that has passed its “sell by date.” What this means in practice is that if something is published in the press, it remains printed and searchable. This ruling is not about re-writing history (as in George Orwell’s horror scenario, “1984”). Everything remains published in the press. If you want to find it you just need to know exactly where to look. In our book example, this would be the page number referenced by the deleted index.

**Replicability**

Digital content can be copied; this means that you can copy personal data from one place and paste it into another place, such as Customer Relationship Management (CRM) sales data copied into the CRM app on a mobile device, or data copied from an approved business system to a USB stick. Copied data is difficult to control, in that it is difficult to determine whether the content has been changed—presenting risks to quality of data.

In the context of personal data collected within your organization, personal data collected for a specific purpose must be used purely for this specific purpose. Personal data collected to deliver a book to a customer cannot be copied and used for marketing.
Invisible data, or the “unknown unknowns”

It is the CxO’s worst nightmare: Where is personal data being collected and processed within the organization? Which employees have copied (replicability) personal data onto mobile devices or USB sticks without even being aware themselves that it is personal data? If you ask for a definition of personal data, many individuals will respond with PII (personal identifiable information) or some simple examples, such as name, address, IP address, or health data. Very few would have any idea that the definition of personal data is any data which can be linked directly or indirectly to a living individual. It is not uncommon that invisible personal data has attained a state of digital immortality (digital persistence) thanks to human nature being what it is and individuals taking a “keep just-in-case” approach over safe erasure.

Unintended processing

The mere act of storing personal data is an act of processing personal data. Everything your organization does with personal data, even the process of backing up data, is processing. Archiving personal data is processing. All personal data is processed in some form or other until it is securely erased from every system.

Privacy is individual-centric!

If you have not worked it out by now, privacy is “individual-centric”! Let’s start with ownership of personal data. Does this really matter? Yes, because by exploring this question you can weed out the real privacy experts from those who claim they are experts.

Who owns personal data?

The answer to this question is fundamental to privacy and data protection principles, not just the GDPR. If you get this wrong, you will get it all wrong. The funny thing is that most IT and information security experts will get it wrong. This is not surprising because they spend most of their working life protecting the intellectual property of their employers and clients, so it would never occur to them that personal data stored by the company (data controller) does not in fact belong to the organization, but to the data subjects themselves.
The data subject in effect loans their personal data to whichever legal entity is required in order to fulfil a specific purpose. You could liken this to lending your car to a friend. You would expect at least the following:

- That your friend would take care of the car, not to scratch or dent it.
- If anything goes wrong that they inform you immediately.
- Your friend would use it only for the purpose they stated at the outset, and if it was used for something more, that they would be transparent that this was the case.
- Your friend would pay for fuel used.
- The car would be returned once the purpose for lending it was fulfilled.

To take another example. If you were to buy a book at your favorite online bookstore, you will share your address with the store so that they can deliver your book. Once the book has been delivered and the purpose fulfilled, the online bookstore should delete your personal data unless you have agreed that they can keep it in their records, i.e. to save you from having to type it in again when you buy another book.
## Learning Activity

For discussion in groups.

<table>
<thead>
<tr>
<th>#</th>
<th>Privacy Foundations</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Iris scanners (biometrics) are used by your organization to permit access to restricted areas that contain radioactive materials. Is biometrics personal data? Provide justification for your response.</td>
</tr>
<tr>
<td>2</td>
<td>The head of security wants to place surveillance cameras in the office space, including the corridors leading to the restrooms. As the Chief Operating Officer, how will you deal with this request?</td>
</tr>
<tr>
<td>3</td>
<td>The FindMyFriends App is available on both iPhone and Android. What are the most probable collection channels used to provide the service to its users? Is the user <em>active or passive</em> in the collection of personal data?</td>
</tr>
<tr>
<td>4</td>
<td>ACME AB has a <a href="mailto:jobs@acme.se">jobs@acme.se</a> address configured to receive applications for a jobs that have been posted on its website. HR has configured this as a group mailbox that syncs the emails received to their local mailbox stored on their PC. As a privacy specialist, do you see a problem with this practice?</td>
</tr>
<tr>
<td>5</td>
<td>Learning Books AB is collecting customers’ names and addresses when they order books online. The marketing department is using this data for a new marketing campaign. As a privacy professional, how would you explain to marketing and management that this is not allowed?</td>
</tr>
</tbody>
</table>
Appendices

Appendix A – GDPR Definitions (Article 4)

(1) ‘personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

(2) ‘processing’ means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

(3) ‘restriction of processing’ means the marking of stored personal data with the aim of limiting their processing in the future;

(4) ‘profiling’ means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person’s performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements;

(5) ‘pseudonymisation’ means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

(6) ‘filing system’ means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;

(7) ‘controller’ means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

(8) ‘processor’ means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

(9) ‘recipient’ means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;

(10) ‘third party’ means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the
controller or processor, are authorised to process personal data;

(11) ‘consent’ of the data subject means any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

(12) ‘personal data breach’ means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

(13) ‘genetic data’ means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;

(14) ‘biometric data’ means personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;

(15) ‘data concerning health’ means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status;

(16) ‘main establishment’ means:

a) as regards a controller with establishments in more than one Member State, the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in
another establishment of the controller in the Union and the latter establishment has the power to have such decisions implemented, in which case the establishment having taken such decisions is to be considered to be the main establishment;

b) as regards a processor with establishments in more than one Member State, the place of its central administration in the Union, or, if the processor has no central administration in the Union, the establishment of the processor in the Union where the main processing activities in the context of the activities of an establishment of the processor take place to the extent that the processor is subject to specific obligations under this Regulation;

(17) ‘representative’ means a natural or legal person established in the Union who, designated by the controller or processor in writing pursuant to Article 27, represents the controller or processor with regard to their respective obligations under this Regulation;

(18) ‘enterprise’ means a natural or legal person engaged in an economic activity, irrespective of its legal form, including partnerships or associations regularly engaged in an economic activity;

(19) ‘group of undertakings’ means a controlling undertaking and its controlled undertakings;

(20) ‘binding corporate rules’ means personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity;
(21) ‘supervisory authority’ means an independent public authority which is established by a Member State pursuant to Article 51;

(22) ‘supervisory authority concerned’ means a supervisory authority which is concerned by the processing of personal data because:

a) the controller or processor is established on the territory of the Member State of that supervisory authority;

b) data subjects residing in the Member State of that supervisory authority are substantially affected or likely to be substantially affected by the processing; or

c) a complaint has been lodged with that supervisory authority;

(23) ‘cross-border processing’ means either:

a) processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State; or

b) processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State.

(24) ‘relevant and reasoned objection’ means an objection as to whether there is an infringement of this Regulation or not, or whether the envisaged action in relation to the controller or processor complies with this Regulation, which clearly demonstrates the significance of the risks posed by the draft decision as regards the fundamental rights and freedoms of data subjects and, where applicable, the free flow of personal data within the Union;
(25) ‘information society service’ means a service as defined in point (b) of Article 1(1) of Directive (EU) 2015/1535 of the European Parliament and of the Council;

(26) ‘international organization’ means an organization and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries.
Appendix B – More on Consent

The legal entity, i.e., organization, whether a public authority or private enterprise, must log consent (legal basis for processing, Article 6(a)) and be prepared to show it as evidence to the data protection authority on request.

There are a number of different types of consent, these are discussed now.

Informed consent

A type of consent which we are all familiar with is when we sign with an old-fashioned pen a “consent” form, maybe concerning the use of our medical or other type of data in the name of research. Nowadays it is more common to find a hyperlink to the privacy notice. Within the form or hyperlink, will be an information giving us information on what we are consenting to. This makes the consent “informed.” Informed consent is required in the GDPR. What this means in your business is that if you are requesting your customers share personal data on your website, you need to provide a link through to your privacy notice, so they are informed on what they are consenting to when they tick the box.

Under the GDPR, consent must in addition be “freely given,” “specific,” and “unambiguous.”

Freely given consent

Consent from the data subject must be freely given. What this means is that the individual should in no way feel pressured to provide consent on the sharing of personal data. There cannot be an imbalance in the relationship between the controller and the data subject. For example, an employee (data subject) is not in an equal relationship with their employer (controller) in the context of their employment. Hence, it is not acceptable for the employer to use consent as the legal basis of processing of personal data shared by an employee. In this context the legal basis is normally Article 6(b), which refers to contract.

What’s more, a controller may not make a service conditional upon consent, unless the processing is absolutely necessary for the service.

In the new regulation, it is not enough to place a tick-box for the data subject to agree to everything. You need to give them options for partial
opt-ins. It is *not* an all-or-nothing approach. So, an example would be that a patient may agree to the collection of their personal data purely for the purpose of receiving a medical diagnosis, but *not* to be used for medical research. You cannot state that in order to get a diagnosis, they must share their personal and sensitive data for medical research. This creates an imbalance in the relationship of consent, which contradicts with “freely given” consent.

**Unambiguous consent**

So, what is *unambiguous* consent? Well, it is defined in the GDPR as similar to *implicit* consent but strengthened “by a statement or by a clear affirmative action.” An example of this could be when the data subject ticks a box on a website or chooses a specific setting. Consent cannot be presumed purely with the act on continued use of the service.

*Implicit* consent is where by the mere act of continued use of a web service you are consenting to the collection of personal data.

**Specific consent**

Consent must be specific; it needs to be described precisely what the data subject is consenting to. The controller cannot request open-ended or blanket consent to cover the possibility of future processing.

Additional processing for archiving data in the public interest, statistical purposes, or scientific and historical research generally will be exempt from specific consent. However, there are strict rules on techniques that should be used for anonymization and pseudonymization of data in order to protect the rights of the data subject.

**Opt-in versus opt-out**

The default option in the collection of personal data under the GDPR is opt-in. What this means is that you cannot place a tick-box on a webpage or a form whereby your customers must tick the box to prevent you collecting their personal data. This is opt-out. The GDPR is very specific that the data subject, who could be your customer, must opt-in before you can collect anything!

It also provides that “the user’s consent to processing may be expressed by using the appropriate settings of a browser or other
application.” However, in this case the browser’s default settings must be to reject the placement of cookies, thereby requiring the user to actively opt-in to receiving cookies.

Withdrawal of consent
The rights of the data subject extend beyond the provision of consent to the withdrawal of consent. The GDPR gives data subjects the right to withdraw consent at any time, and it must be easy. In fact, the GDPR states that the withdrawal of consent should be as easy as giving consent. Once the data subject has withdrawn consent they have the right to have all their personal data collected erased, and it should no longer be used for processing, unless the controller can continue the processing on the basis of another legal ground.

Explicit consent
Explicit consent requires a signature, or an explicit action from the data subject, such as ticking a box before or upon the sharing of personal data. GDPR requires explicit consent for special categories of personal data. Sensitive data includes data “revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation.”

Parental consent
GDPR requires explicit parental consent for processing children’s personal data, when the child is under the age of 16 years old. Each EU member state has the option to reduce the minimum age to 13 years.

Controllers must make “reasonable efforts” to verify that a parent or guardian has provided the appropriate consent. Now as for what this means in practice, we can only look to the Children’s Online Privacy Protection Act (COPPA)\(^1\) in the U.S for guidance.

---

Consent to profiling

Controllers need to obtain *explicit* consent in order to make decisions about the data subject using automated techniques. An example of this is profiling. This is most important when the effects of an automated technique, such as profiling, can impact on the rights of the data subject.