PRACTICAL

GUIDE

1ste edition 2018

PRACTICAL GDPR GUIDE

THE NEW EUROPEAN PRIVACY LAW

Author: Viktor D'Huys, Group Joos

Co-author: Peter Witsenburg, Belgium Cloud & CloudMakelaar

Table of contents

Foreword

A little while ago, I came across the following line in an article: "Money no longer makes the world go around, data make the world go around." There is a good case that can be made for that view. The impact of data on our lives continues to grow. Besides providing the chief fuel for the new digital economy, data are also steering our lives through new technologies to a growing extent.

Just to be perfectly clear, that is a good thing. Our personal lives, social lives and society have been improved by smart devices and applications. From the apps on our smartphones to new technologies in smart cities, data help us to advance. The applications are endless, and include seamless mobility, improved air quality and customised healthcare.

Personal data have become the new El Dorado thanks to the faith people have in such information. It is in huge demand among developers because they believe personal data will be able to offer solutions for the problems we face today. More and more of what we do is being recorded, and recent years have seen a dramatic rise in the digitalisation, storage, processing, dissemination and exchange of massive amounts of personal data.

This has inevitably created risks when it comes to protecting the privacy of individuals. Data protection is now a greater challenge than ever before. It presents us with a fundamental question: how do we guarantee that private individuals are in control of their personal data, and at the same time allow the digital economy and digital entrepreneurs to continue to flourish?

The General Data Protection Regulation is Europe's answer to this question. It recognises that the interests of developers and citizens are not opposed and in fact coincide to a great extent. Private individuals are concerned about their privacy, but they are also looking for new, often personalised, applications that improve their lives. And while businesses are looking for data, they can use to develop their products, they are also increasingly aware that their customers are concerned about privacy issues.

The chosen solution is therefore clear: stronger protection for, and a greater appreciation of, personal data in a European digital single market. We have achieved this by harmonising the 28 different practices existing within the European Union. This means businesses need to comply with only one piece of legislation. This ensures personal data can be exchanged more efficiently and also provides a boost for innovative digital applications for everyone in Europe.

At the same time, processors of data have to handle the personal data of their new and existing customers in a responsible manner. It is up to the relevant data protection authority to monitor compliance with data protection legislation. It does this by providing businesses with guidance and coaching on how to comply with the new legislation. In this context, sanctions are a last resort and are never a goal in themselves.

All of this will lead to a greater appreciation of our personal data. After all, the aim of the European digital strategy is to ensure businesses handle our valuable personal data in the most efficient way possible. Personal data form the engine behind the booming digital market, where the limits of technical progress are pushed back on a daily basis. It is crucial that all businesses analyse and optimise their data processing so that they can unlock their full potential.

The new legislation achieves its dual objective by providing for measures that ensure the basic right to privacy remains protected in the digital age, while giving businesses in the digital market full scope to develop their products. There is one crucial group of players that we must not overlook in all this: the organisations that are dedicated to informing businesses and private individuals about this new legislation. These include Group Joos and CloudMakelaar, the organisations behind this book. As the Secretary of State with responsibility for privacy, I am extremely grateful to them.

I hope you will enjoy reading this book.

Philippe De Backer

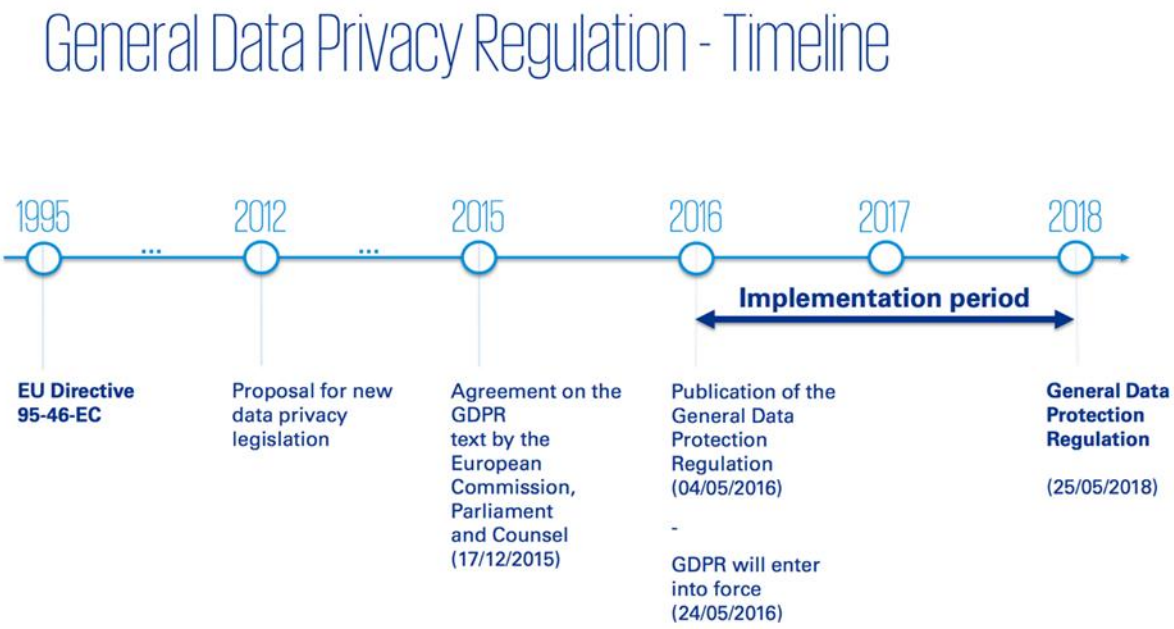
Belgian Secretary of State for the Fight against Social Fraud, the Protection of Privacy, and the North Sea.

GDPR: New rules, new challenges

Since May 25, 2018 the General Data Protection Regulation (GDPR) is in place. GDPR, officially the Regulation (EU) 2016/679 of 27 April 2016, is an EU regulation of 88 pages with 99 articles and 173 ' Considerations '. It applies to any person or organization that collects or processes personal data in the EU or outside the EU but on people who live in the 28 Member States of the European Union or non-Europeans who are in the EU. By extension it also applies for the non-EU countries participating in the European economic area (EEA) (Iceland, Norway and Liechtenstein).

What new rules the GDPR introduces and, more importantly, what does this mean for your company? There is, of course, nothing new about data protection legislation. The right to privacy and the collection and use of personal data by companies have given rise to tensions ever since the Universal Declaration of Human Rights was adopted in 1948.

The arrival of the internet and big data has made it necessary to find a new balance. This is where the GDPR comes in. The EU is introducing this new set of rules to ensure uniform legislation throughout Europe.



Moreover, the rules will become much more stringent, and this will have major consequences, especially for companies that collect and use personal data on a large scale or as their core business.

First of all, the personal data stored by your company must be well protected. Examples include encrypting data on your website, storing data in properly secured locations and being transparent about which people within your company are authorised to access data.

You will also have to be transparent about which data you store, how you use data and the purposes for which this is done. For example, visitors to your website need to give their approval for their data to be used for purposes which are announced in advance. They need to know which data you keep and what you do with the data. In addition, everyone needs to be able to view and change their own data and have data deleted where appropriate. Complying with these obligations is obviously a major task.

Finally, you need to have a contingency plan that can be put into effect in the event of a data breach. In some cases, the data breach will also have to be reported to the supervisory authority and even to affected individuals. Moreover, all the rules also apply to all companies that have an involvement, including subcontractors.

We will provide relevant information and a range of hints and tips for dealing with the introduction of the GDPR in the next chapters of this book.

1. Definitions

1.1. What does the term 'personal data' refer to?

It is impossible to discuss the GDPR without reflecting on the definition of 'personal data'[1]. The GDPR defines personal data as "any information relating to identified or identifiable natural persons". As with all definitions, every word matter, and so each of the terms contained in the above definition is considered separately below.

- Natural persons:
  The definition of personal data encompasses data about private individuals who are still living, but not data concerning legal entities. It therefore excludes companies that are clients or suppliers, although it does include the details of contact persons, for instance.
- Identified persons:
  A person may be identified by means of their surname, first name, address and date of birth, for example. The more data you have collected and the smaller the group of people concerned, the easier it is to trace information back to one individual.
- Identifiable persons:
  Data that cannot be linked to a person may contain a key that allows the data to be combined with other data. If this could result in the identification of an individual, the data concerned are personal data. The GDPR explicitly states that such data will continue to be classified as personal data so long as it is possible to combine the data by making reasonable efforts.
- Any information:
  This term clearly indicates that the data in question are not restricted to digital information contained in databases, and that personal data also include data collected on paper, visual materials, sound recordings and other information. Some of the previous legislative initiatives were limited to digital information, but this is specifically not the case when it comes to the GDPR.
- Information relating to a person:
  Information that, on its own, indicates nothing about a person can still be considered personal data if it is linked to a person. Examples include location information (i.e. information indicating a person's location at a particular moment).

[1] Article 4.1 en 4.6 : Recital 15, 26-27 en 30-31

The term 'personal data' therefore covers a vast array of data, including your name, address, date of birth, marital status, and partner's and children's names, the medical file kept by your GP and a list of any criminal convictions. You no doubt often make information about your qualifications, knowledge of languages and work experience available on purpose. You probably share personal experiences on social media with friends and family only, and keep them screened off from the outside world. However, have you ever considered data such as the list of all the items you bought in your favourite supermarket during the past year, or your internet search history? Personal data even include the precise location of your mobile phone (and therefore most likely your own location) at various times.

Tip:

To gain an idea of the amount of data that comes within the scope of the GDPR, try listing all the personal data you come across in your own working environment and all the data that your employer or business contacts at other companies are likely to hold about you. Complete this exercise before reading further.

Have you finished your list? Did you give any consideration to the following items?

- Drawers full of business cards, or spreadsheets containing contact details
- The home telephone numbers of your colleagues, or the direct number of a consultant that you were given in confidence for use in an emergency
- Photos taken during the most recent staff party
- Your CV
- Evaluation or appraisal interview reports
- Records of days worked, absences and sick leave
- Camera images taken at entrances to business premises or in the workplace
- Logs that the IT department keeps of the hours you are logged on to the network or specific applications, as well as the websites you visit.
- Your email messages (their content, the number of messages and the recipients)
- Questionnaires you complete in order to receive information from a supplier, download a white paper or sign up for a newsletter (e.g. your areas of interest, your hobbies, your position within your company, and how much experience you have).

Although this list is by no means exhaustive, it clearly shows why legislation is needed to ensure that all those who use personal data handle such data with due care and adhere to a number of rules. At the same time, it is also inevitable, and even necessary, that personal data can be used by private individuals, the government and even businesses. The GDPR seeks to ensure a good balance is found between an individual's right to privacy and the possibility that businesses may make cross-border use of the wealth of data that is available.

This book will explain how the GDPR seeks to strike a balance between these two perspectives. The kind of data used, and the intended purpose are of crucial importance when determining the obligations that have to be fulfilled.

The next chapter of this book will therefore take a closer look at the different levels of sensitivity that apply to personal data and what the law refers to as ‘special categories. Afterwards we go on to consider the precise definition of data processing and the related roles and responsibilities.

1.2. Special categories of personal data

The GDPR seeks to find a balance between the purposes for which organisations collect and use personal data and the right that all individuals have to the protection of their privacy. The nature and quantity of the processed data must always be proportionate to the purpose for which the data are used.

The extent to which personal data are sensitive varies widely. Some personal data are publicly known or are so widespread and easy to find that a data breach would cause hardly any problems and could not be considered a true invasion of privacy. Other types of data are so confidential that the GDPR has created special categories of personal data, to which additional rules apply. It is therefore crucial that you are aware from the outset whether the personal data that are to be processed belong in a special category[2].

The GDPR specifies the following special categories:

- Information about a person's racial or ethnic origin
- Data relating to a person's religious or philosophical beliefs
- Information about a person's political opinions or trade union membership
- Data relating to a person's sex life or sexual orientation
- Medical information
- Biometric identification data and DNA
- Information about criminal convictions and offences

The Belgium Data Protection Authority (GBA) provides the next example listing.

[2] Article 4.13-15; Article 9-10 : Recital 34-35 en 51-56

Personal Data Categories (Privacy Commission)	Personal Data Category?
A. Identificatiegegeven B. Financiële bijzonderheden C. Persoonlijke kenmerken D. Fysieke kenmerken E. Leefgewoonten F. Psychische gegevens (informatie over karakter en persoonlijkheid) G. Samenstelling van het gezin H. Vrijetijdsbesteding en interesses I. Lidmaatschappen K. Consumptiegewoonten L. Woningkenmerken N. Opleiding en vorming O. Beroep P. Rijksregisternummer / Identificatienummer van de sociale zekerheid V. Beeldopnamen W. Geluidsopnamen	"Regular" Personal Data
J. Gerechtelijke gegevens M. Gegevens betreffende de gezondheid Q. Raciale of etnische gegevens R. Gegevens over het seksuele leven S. Politieke opvattingen T. Lidmaatschap vakbond U. Filosofische of religieuze overtuigingen	Special Category

As a general rule it is best not to collect or process any of the above data. However, if such data have to be collected and processed, the purpose for which, and the legitimate ground on which, this is done must be clearly recorded. Specific conditions have to be met for those special categories. When it comes to the different phases of data processing, stricter standards also apply with regard to information security, transfers of data to a location outside Europe, and the handling of data breaches in particular. We will therefore revisit this subject in future sections of this book.

With regard to personal data that do not belong in any of the special categories, it is still possible to make a distinction between data that have a low risk of invading privacy and more sensitive information. Financial information, for instance, is more sensitive than an address, and data concerning children must always be handled with extra care.

If you collect and use personal data, you must therefore always consider whether you really need the data in question for your intended purpose and how great the risk is that a person's privacy may be invaded. The risk increases in line with the number of people concerned and the amount of data collected on them. This is essentially how the privacy impact assessment (PIA) is performed. An entire project may need to be set up for the PIA, or, depending on the circumstances, a simple weighing-up of the facts may be sufficient, but you always have to keep record.

In addition, a number of steps can be taken to reduce the sensitivity of the personal data that are to be processed.

The best solution is using anonymous data. If the data have been correctly anonymised (meaning that the individuals cannot be identified any more), they no longer count as personal data and therefore the GDPR does not apply. Data used for academic research are always anonymised wherever possible, and this approach is also suitable for large scale data processing for marketing purposes. One of the methods that may be used is to combine data to form groups.

If this method is chosen, the amount of data must be large enough to ensure each group always contains a reasonable number of individuals (a minimum of 50 people often applies). You need to be aware that the wider the variety of data you collect, the more likely it is that a person will be identifiable if data are combined.

One commonly used method is pseudonymisation[3]. In this method, all the elements in a dataset that identify an individual are removed and replaced by a meaningless key. The file containing the keys is stored separately.

[3] Article 4.5; Article 25 : Recital 78

Although such data still qualify as personal data, because they relate to an identifiable person, the risk that there will be an impact on any of the persons concerned is much lower. Pseudonymisation is therefore a good security measure for sensitive data that have to be transferred, for example.

Although the definitions used in the GDPR for personal data, sensitive personal data and personal data that belong in special categories are essentially the same as those used in the old privacy legislation, a good understanding of them is needed as a starting point whenever the impact of the GDPR is considered. The next chapter of this book will offer a more in-depth examination of what is meant by processing itself and of the roles that the law recognises. In that field there are significant differences between the GDPR and former rules.

1.3. Data processing and related roles

In order to assess what the GDPR will mean for your own business or job, it is not enough to know which data are classified as personal data. You also need to have a good understanding of what the law means exactly by the term 'data processing[4]'. It is also important to be aware of the different roles that parties play in the processing of personal data. This is because the role you play determines your responsibilities and obligations to a large extent.

Data processing

Data processing must be viewed in very broad terms. Obviously, it includes collecting data about contact details, interests, purchasing behaviour and website visits. Such data are used in marketing or sales campaigns.

However, data processing includes much more than that. The actual activity does not matter: any activity involving personal data is a form of data processing to which the GDPR applies. Looking up and viewing data, storing data, deleting and erasing data, and transporting data are just some of the activities that are considered data processing under the law.

It is important to interpret data processing sufficiently broadly when compiling lists of data processing activities that are performed in-house or entrusted to third parties.

[4] Article 2.1-2; Article 4.2

A firm which provides payroll services to third parties obviously processes personal data, but so does the supplier which collects waste paper from your business if that waste paper includes personalised documents containing personal data.

The private use[5] of personal data by individuals does not, however, come within the scope of the GDPR. Neither does the work of the courts and the law enforcement agencies, as their work is governed by different legislation.

The roles

Privacy legislation identifies a number of roles with respect to data processing. The most important roles are those which the GDPR defines as the 'Data Controller' and 'Data Processor'.

The **Data Controller**[6] is the party that takes the initiative to collect (or arrange the collection of) personal data and keep such data, with the intention of processing the data in some way.

The Controller must record the specific purpose of the data processing and demonstrate that it has legitimate grounds for this. It must decide in advance which personal data are required in order to fulfil that purpose. From a legal perspective, it is crucial that the data collected and processed is restricted to what is necessary for fulfilling the purpose. This is because not processing data is the best way to protect privacy. The Controller also guarantees the security of the collected data.

The Controller ensures that the data are available, that their integrity is maintained at all times (i.e. that they are not wrongly changed or erased) and that there are no breaches of confidentiality. A crucial aspect in this context is that the data must be used exclusively for the purpose for which they were collected.

[5] Article 2.2c : Recital 18
[6] Article 4.7

The role of **Data Processor**[7], by contrast, involves acquiring personal data from the Controller and processing the data in accordance to the Controller's instructions, depending on the purposes for the processing. The Controller can take on this role, of course. If the Controller decides to use a third party, however, the third party will only play the role of Processor. This fundamental distinction forms the basis for the statutory obligations. Crucially, the GDPR, in contrast to previous privacy legislation, also imposes explicit obligations on the Processor.

It is important to realise that clearly defining the allocation of tasks is not always easy. For example, it is perfectly possible that a Processor may collect the personal data. This is because a Controller is able to instruct a Processor to collect, enrich and analyse personal data as part of its work. These are all examples of what the law means by the 'processing of personal data'.

The fact that a party collects data does not automatically make it the Controller. Conversely, the client of a Processor remains responsible for the data even when the data collection activities are outsourced to the Processor.

[7] Article 4.8

In future, it will be necessary to have a contract that clearly sets out the roles that the client and contractor play in data processing. It is a good idea to make sure this matter receives constant attention. The new law assumes that data processing always takes place in the context of a data processing contract that clearly sets out the mutual obligations with regard to data privacy. However, you need to be aware that your responsibilities are related to the role you actually play, regardless of whether this role is covered by a contract or not. This means that as Processor you need to make sure you do not assume any responsibilities that are not in keeping with your role. The most important and obvious restriction is that you must never use the data that the Controller has entrusted to you for any purpose other than the purpose specified in the Controller's instructions.

Finally, the law clearly defines a third role, that of the **Data Subject**[8]. The Data Subject is the individual to whom specific personal data relate. It is principally the Data Subject who enjoys legal protection under the law. The GDPR explicitly gives Data Subjects a number of rights concerning their personal data. These rights are fundamental to the new Regulation. First, the GDPR requires that Data Subjects are given clear and transparent information on the processing of their data.

In addition, they also have the right to what is usually summed up as 'fair use' of the data. This encompasses the legal acquisition and processing of the data as well as taking care to ensure the data remain accurate, are adequately protected and are only used for the stated purpose. Data Subjects are entitled to receive information about all these aspects. Finally, Data Subjects are, to a large extent, able to control their individual data (they can retrieve, correct and erase their data and stop their data from being processed).

The rights and duties associated with each role will be discussed in detail in a future chapter of this book.

[8] Article 12

1.4. The Data Protection Officer

This chapter of our book looks at the types of companies that require a Data Protection Officer[9] (DPO) as well as the role that the DPO plays.

The GDPR does not require that every controller designates a DPO. For a long time during the preparatory discussions, it seemed likely that the obligation to designate a DPO would apply to all companies with at least 250 employees, but this goal was eventually abandoned. The obligation is now based much more on the nature of the business. If an organisation's activities carry a real risk of serious infringements of privacy, owing to the amount of data processed, the nature of the data or the frequency of the data processing operations, the organisation must have a DPO to ensure it complies with the legislation. Certain organisations are always required to designate a DPO. This group consists of all government organisations, all companies whose core activities consist of processing special categories of personal data, and all companies or organisations whose core activities consist of regularly and systematically collecting and processing personal data on a large scale.

Even if you are under no legal obligation to do so, it is recommended that you explicitly assign the role of DPO to a specific individual, as this will ensure your company has designated a person to lead the preparations. The DPO will ensure there is a culture of data protection within your company, that the topic of data privacy is placed on the agenda and that your company is ready for the GDPR in time. The DPO will have to be given sufficient time to study the legislation and learn the ropes, after which the knowledge gained can be passed on to the rest of the organisation. And it goes without saying that the DPO plays a leading role in the GDPR project.

[9] Article 37-39 : Recital 97

Requirements applying to the Data Protection Officer

Companies that have to designate a DPO must take a number of requirements into consideration. The DPO's name and contact details must be reported to the Data Protection Authority.

The DPO must have expertise in the area of privacy legislation as well as a thorough knowledge of the company, its activities and the market in which it operates. He or she must also have sufficient authority and be given adequate resources to perform their task.

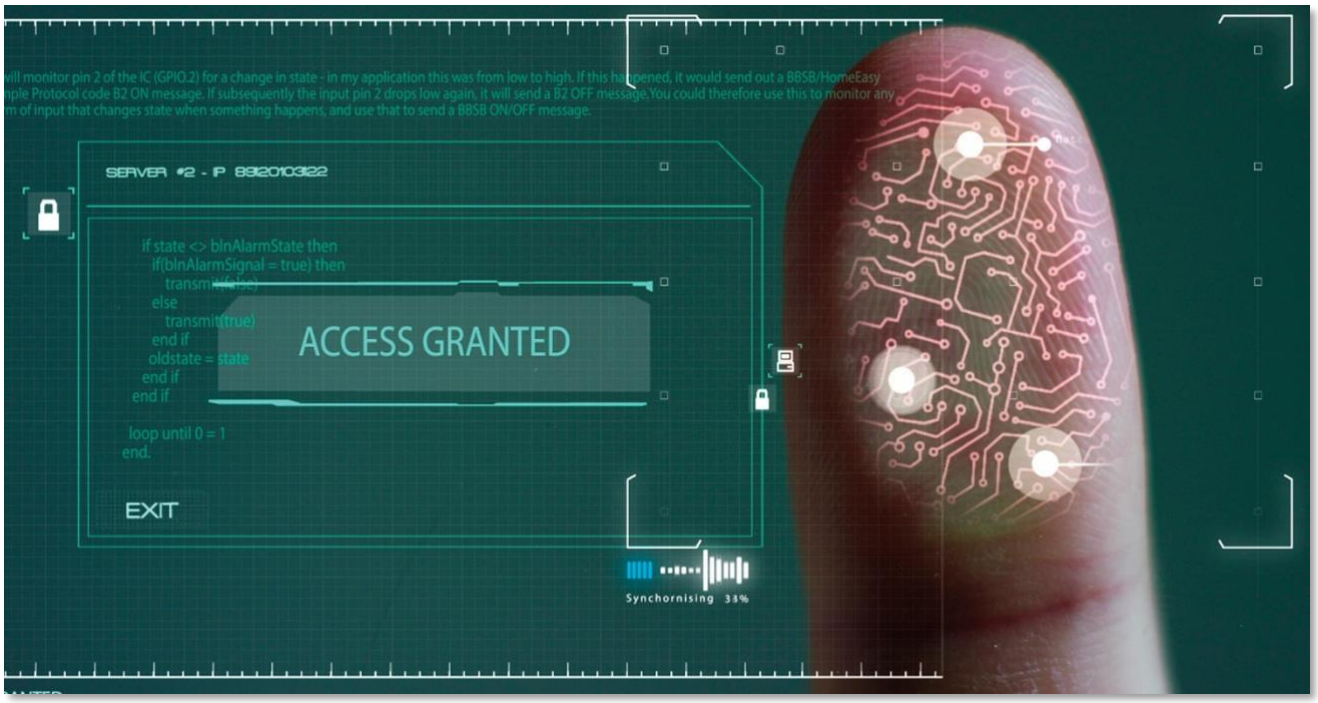
The DPO is expected to report to senior management and therefore be sufficiently independent. Moreover, no conflicts of interests may arise. For this reason, a person with responsibilities in the area of IT will usually not be able to hold the position of DPO at the same time, since that person would have to check the security measures set up by their own team. The way in which the position of DPO is filled in practice depends of course on the scale of the organisation. At small companies, the role of DPO will not be a full-time position and so can best be combined with other tasks. It is also perfectly possible for an external person to perform the role of DPO.

The GDPR does not specify any qualifications or certificates that must be held by the DPO, nor does it indicate whether precedence is to be given to legal, organisational or technical knowledge and experience. Obviously, a certain amount of knowledge is required as a minimum even at small organisations. Besides the efforts put into accumulating knowledge, which can be made in a wide variety of ways, it is also worth investing in a few days of specific training.

A DPO confers an advantage

Having a DPO therefore confers a significant advantage, even if you are not legally required to have one in your specific situation. The DPO plays a role in each of the six preparatory steps that were identified in the fourth chapter of this book.

The DPO also has important tasks to perform in other procedures relating to personal data. He or she is involved in setting up all new personal data processing operations and provides advice on risks and the data protection measures that are required. The DPO is also involved in following up incidents and data breaches, and in this context is the first point of contact for clients, data subjects and the supervisory authorities. Finally, one of the primary tasks of the DPO is to guarantee the rights of the data subjects. In this context, the DPO acts as the direct point of contact for data subjects. We will therefore come across the DPO again many times in future chapters of this book.



2. The basic principles of GDPR

This chapter looks at the basic principles of the GDPR[10] and the resulting obligations that you, as the controller, must fulfil with regard to the processing of personal data. It also includes six steps you can take to ensure you are compliant

Fair use of personal data

The GDPR seeks to create a regulatory framework that enables businesses and organisations to make use of personal data and at the same time guarantee the privacy of data subjects wherever possible.

The basic principles governing the legitimate use of personal data are as follows:

- you must be transparent about the data you keep and the processing operations you carry on;
- the data must be processed in a manner that is lawful and fair;
- the rights of the data subjects must be guaranteed;
- the confidentiality and integrity of the data must be respected;
- the controller's liability must be established.

These principles are not new to privacy legislation, and over time they have come to be defined in a more systematic, clear way.

The most important obligations that controllers have to fulfil under the GDPR stem directly from these principles.

- Transparency is achieved by being clear about the personal data you keep, the type of processing you carry on and the objective you wish to achieve by processing the data. Information covering this must be easily accessible and be written in clear, straightforward language that can be understood by all.
- The fair use of personal data means that the data must be acquired in a lawful manner, that you must use it exclusively for the set purpose, and that the amount of data collected, and the length of time for which the data are kept, must not exceed what is necessary in order to achieve that purpose.
- Every data subject has a right to information concerning the way in which you process their data. They may ask to inspect their individual data and may have the data corrected, supplemented or removed. In certain circumstances, a data subject may stop their data from being processed. Ensuring all these rights are respected is not an easy task.

[10] Article 5 : Recital 39

- Respecting the data means you must do everything possible to ensure the data are entered correctly and kept up-to-date and secure, so that they are not wrongfully published or used for the wrong purpose.
- The controller must be able to demonstrate that it complies with all its obligations under the regulation and is liable for any shortcomings.

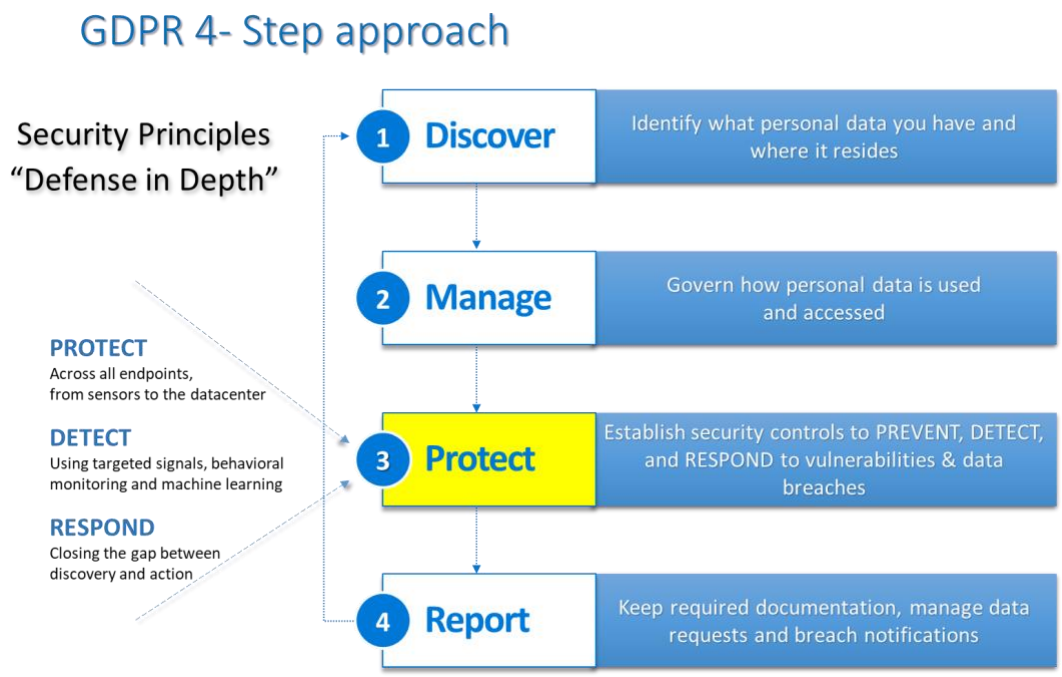
These objectives will obviously be fully supported by all those who recognise the importance of corporate social responsibility. The GDPR and the more detailed explanations supplied by the national supervisory authorities (in Belgium this is the Privacy Commission) should therefore be considered as a help, rather than a way of imposing privacy constraints, as companies and other organisations can use these documents as a guide for achieving important goals while continuing their current activities.

Being compliant with the GDPR

The most important steps that data processing controllers have to take in order to ensure compliance with the new regulation are briefly summarised below.

- Set up **records of processing operations involving personal data**. This is an obligation under the GDPR, and you must be able to present these records to the Data Protection Authority when you are asked to do so. You should primarily consider this to be a useful resource for yourself. This is because the records will provide you with a picture of all the personal data that you use. The records must state the type of data concerned, the type of processing involved, the purpose for which the data are processed and the legal grounds for processing the data.
- Prepare **a privacy statement**. This must be easily accessible wherever you collect contact details and other information about individuals.
- Check whether you have **adequate security** for all the personal data you collect. Is your network secure? Do you encrypt your files that contain personal data or use password protection? When data are no longer required, are they safely removed? (This applies to both digital data and data in printed form.)

- Draw up instructions that set out **what** needs to be done **if a data subject contacts you in order to exercise their rights**, to ensure that you can take the necessary action in time. Who will receive the request? Who will do what?
- Draw up a clear **procedure** containing all the steps to be taken **if a data breach occurs** and there is a risk that the privacy of data subjects could be infringed. Are all of your employees aware of this procedure?
- If you hire in **third parties** to process personal data, ensure there is a **contract** in place that clearly describes exactly what the subcontractor has to do and what its obligations and responsibilities are under the GDPR.



Each of these action points will be worked out in detail in future chapters of this book, in which a general discussion will be accompanied by practical tips.

3. Records of personal data processing operations

3.1 Assessment of personal data and obligation to keep records

The best way to start working on ensuring compliance with the GDPR is to make a proper assessment of the personal data that your company or organisation keeps and uses. It may be the case that you also have to convert this information into formal records[11] of personal data processing operations. It can be difficult to determine whether such records are compulsory in your particular situation. For this reason, in this chapter we will attempt to provide clarification.

Assessment of personal data

Large organisations use specialised software for assessing their personal data, although a simple spreadsheet that contains the necessary information can be just as useful.

Tip:

You can find out a great deal simply by asking the departments involved the following questions:

- Which personal data do they collect and/or use (categories of data, the types of people to which they relate, the number of data subjects involved)?
- How are the data processed (what is done to the data) and for what purpose is this done?
- With which suppliers, partners or other third parties are data shared?
- Are there any flows of data to countries outside the EEA?

Next, you need to determine whether the objective for which the data are used is legitimate and in balance with the data subjects' right to privacy. Finally, you need to identify the threats that exist with respect to guaranteeing the confidentiality and integrity of the data and the measures that you take in order to protect the data.

[11] Article 30 : Recital 82

It is a minimum requirement that every controller responsible for the processing of personal data asks itself these questions.

The output of this exercise will provide you with most of the information you require to set up records of your personal data processing operations, which is a new requirement imposed by the GDPR.

Records of personal data processing operations

The former privacy legislation included an obligation to report automatic processing operations involving personal data to the supervisory authority. In Belgium, this authority was the Commission for the Protection of Privacy (CPP), which is usually referred to simply as the Privacy Commission.

This information was entered in public records that could be viewed by anyone. However, this requirement did not apply to the most common uses of personal data, such as personnel management, payroll records and accounting, customer and supplier management, contact details (as long as these did not include any additional information), lists of members of associations, and student records. As a consequence, the majority of organisations were not required to report any information.

This will be changed since the GDPR entered into force and controllers have to keep their own data processing records. These records must be in digital form, and it must be possible to present them quickly and easily when an audit is carried out by the Data Protection Authority or in the context of an investigation into a complaint or data breach. The records must demonstrate that the controller has a clear overview of the personal data that it processes. The controller uses this to prove it has thought about its right to carry on the processing operations and that the security measures put in place by the controller are adequate.

Another difference between the GDPR and the former privacy legislation is that the GDPR is not limited to automatic data processing and does not provide an exception for 'commonly used personal data'.

Who does the obligation apply to?

An exception to the obligation to keep records[12] can be made for small organisations to a certain extent, although the GDPR is not entirely clear on this matter. For this reason, the Belgian Privacy Commission published detailed recommendations (on 14 June 2017). The most important recommendations are summarised below.

[12] Article 30.5 : Recital 13

- Every controller (and processor – of which more later), irrespective of whether it is a company, government organisation, association or natural person, must keep records of its personal data processing operations.

- An exception is made, however, for organisations with fewer than 250 employees (and with turnover of less than EUR 50 million).
  This is not in keeping with the spirit of the law, however, as all measures must result from the risk assessment. When a small organisation processes personal data, this can entail just as much risk, if not more. For this reason, there are a great many situations in which the obligation to keep records will remain in force, including for SMEs.

- The obligation to keep records cannot be avoided if:
  - the data that are processed concern special categories of personal data or data relating to particularly vulnerable groups of people, such as children;
  - the processing of the data entails risks for the rights and freedoms of individuals and may therefore result in serious physical, material or non-material damage. The recommendations contain a number of examples: if there is a risk that the confidentiality of financial information or data protected by a legal obligation of professional secrecy could be breached, if there is a risk of identity theft or fraud, or if data about health, personality, behaviour or movements, etc., is used to produce personal profiles;
  - the data subject does not have the possibility of exercising their personal rights and therefore has no control;
  - a controller processes the personal data on a structural basis, rather than an occasional basis, in other words the data processing is not an accidental or once-only occurrence but is in fact 'normal'. The example provided in the recommendations refers to information concerning clients, suppliers and employees.

Clearly, drawing a dividing line is very difficult. Every organisation holds some data that could cause damage if there were a breach of confidentiality, and every organisation keeps some data on a structural basis. The Belgian Privacy Commission therefore recommended that all companies and organisations keep records, although in the case of SMEs such records may be limited to the data that is processed on a structural basis. This means that the exercise will be relatively limited in scale at small companies and organisations.

What the records should look like, and what information they need to provide on each processing operation, will be discussed in the next chapter of this book.

3.2. Records of personal data processing

This chapter takes a closer look at the content of the records of personal data[13] processing operations. All controllers would do well to keep such records, even though, strictly speaking, small organisations are not always required to do this.

First of all, you need to draw up a simple list of the personal data that your company or organisation works with. The Belgian Data Protection Authority explains the requirements that the records need to meet, which it has grouped together based on six simple questions (Who? Why? What? Where? Until when? How?). Their website contains a short summary, a detailed paper and a model register, all of which can be downloaded. However, they are not available in English. The six questions are considered below.

Who?

First, your records must establish who the controller is. This means they must contain accurate information about your firm or organisation (including contact details) and the name and details of your Data Protection Officer. If you do not have a Data Protection Officer, your records must identify the person who is to be contacted in the event of any questions, problems, complaints or data breaches. Large organisations are advised to specify the department or person responsible for individual sets of personal data. This is because the department or person in question will act as the point of contact for information about other matters to be included in the records.

Why?

It is essential that you specify the purpose for which you use personal data. The basic principle underlying all privacy legislation, and the GDPR in particular, is that information may only be collected and processed if this is strictly necessary for the intended purpose. Obviously, you require contact details in order to communicate with your customers and suppliers. In addition, your company has to collect names and addresses for its sales and marketing activities. Moreover, enriching basic data of this kind with additional information, such as the geographical distribution of customers or the sectors in which they are active, is also desirable.

The Belgian Data Protection Authority stresses that the purpose must be described in the most specific terms possible and clearly demonstrate the necessity of processing the relevant information.

[13] Article 30.1 : Recital 39

Its paper includes an appendix containing a list of purposes and more precise descriptions that can be used as a tool.

It is also a good idea to consider the legal grounds your organisation has for processing the personal data, although it is not strictly necessary to include this information in the records. In some cases, these grounds will give rise to specific obligations or procedures that need to be followed. You should add that information to the records immediately as it will make it easier for you to check later whether you comply with all the statutory obligations.

What?

Next, you need to record the categories of data subjects (e.g. your customers, employees or visitors) that form the source of the processed personal data that are used for each separate purpose. At this point you also need to indicate the approximate number of data subjects, as this can provide you with an idea of the impact in the event of a data breach.

You then need to specify the information about the data subjects that you keep and use. For example, do you only keep and use names and addresses, or do you also collect information about the data subjects' age, gender, position and interests? A list of possible categories can be found in the appendix to the Privacy Commission's note.

It is crucial that you explicitly state whether certain information belongs in any of the special categories (see chapter 1.2 of this book). This is because special rules and restrictions apply to such information. It is also necessary to identify explicitly any information that does not belong in these special categories but can still be considered sensitive, such as financial information or data related to minors.

Where?

For each identified purpose, the records also need to specify the recipients of the processed information. It may be sent to a natural person, or to a government institution or an internal or external processor. All recipients need to be identified by name.

It is important to indicate whether the information will be processed exclusively within the European Economic Area. If data end up outside the European Economic Area, you need to guarantee that the personal data will continue to be adequately secured and that the data subjects will still enjoy the same rights and protection. This must be demonstrated in the records.

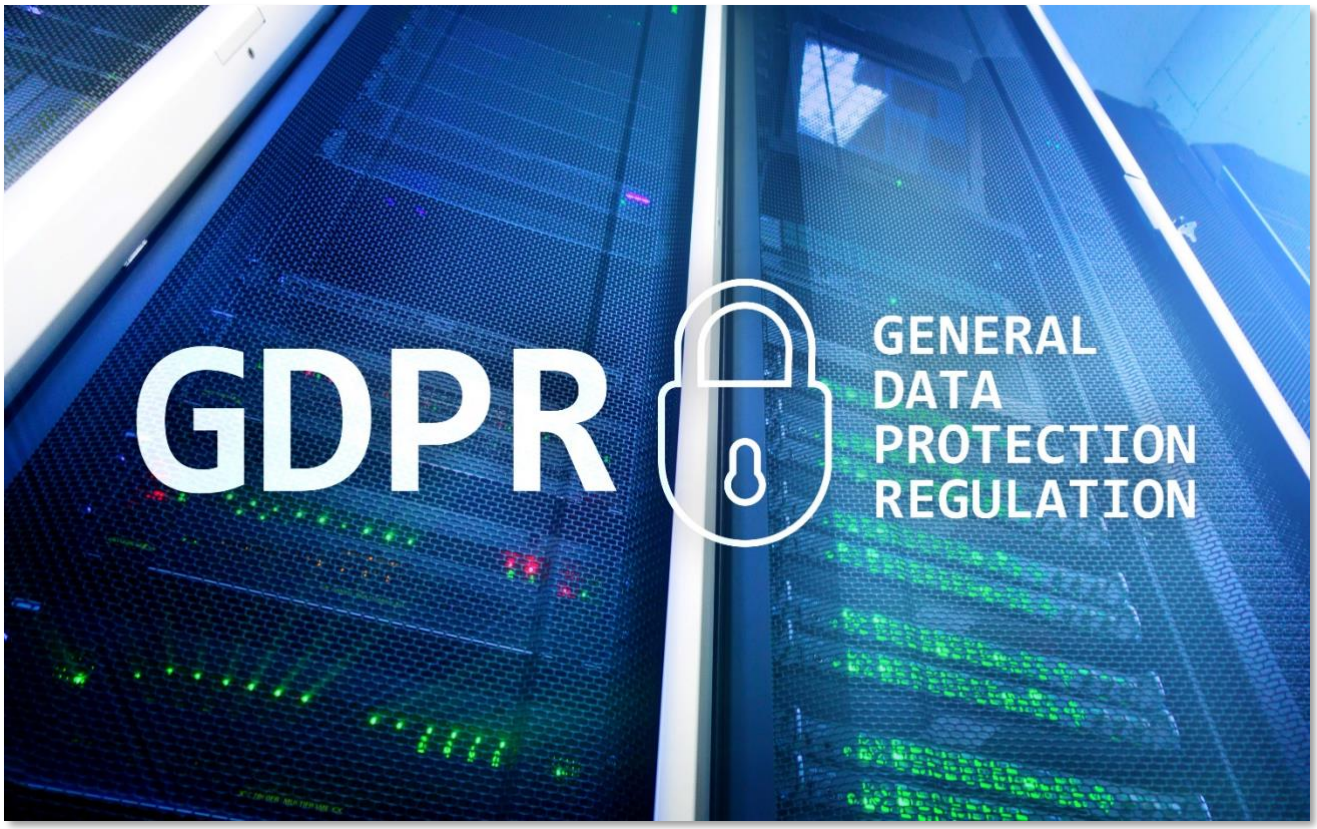
Until when?

As data may only be used for the intended purpose, it logically follows they may not be kept for any longer than is necessary for that purpose. The Privacy Commission has stated that retention periods do not always have to be expressed as a specific number of days, months or years, and formulations such as 'the retention period prescribed by law' are also possible.

How are the data protected?

As a controller, under the GDPR you are responsible for the protection of the personal data you process. You need to take all necessary measures to ensure their confidentiality and integrity are not compromised. The data must not be wrongfully published or passed on to the wrong recipients, and they must not be wrongfully altered.

Maintaining complete, accurate records will provide you with a good basis for demonstrating that you exercise due care when processing personal data and that you take your responsibility seriously. It will also provide a starting point for working out your own internal procedures and checking whether these procedures are applied correctly. And, finally, it will also prove helpful when you draw up privacy statements.



4. Legal basis for processing personal data

4.1 Legal basis for processing

When preparing records of personal data processing operations, it is advisable for controllers to document the legal basis[14] in the records although this is not a requirement. In order for the data to be used legally, the processing operation must have a specific purpose and a demonstrable legal basis. Moreover, the processing operation must comply with the rules on subsidiarity and proportionality, which means it must be necessary and be proportionate to the purpose.

The GDPR provides for a number of potential legal bases, which are not applicable in all cases. Before you start a processing operation, it is important to carefully consider your legal basis. This procedure must be documented and may play an important role later on in the event of any disputes or complaints.

The clearest, most specific instructions provided by the GDPR in relation to the legal basis concern **the data subject's consent**, which we will discuss in detail in the next chapter of this book.

Other legal bases can also be relied on. **The data may be required for the implementation or preparation of a contract**. All sorts of personal data are required in the context of the relationship between a customer and a supplier, first and foremost of which are contact details, but in the B2C world payment data and financial information are also frequently required. This legal basis provides adequate justification insofar as the processed information is demonstrably required in order to conclude the contract or provide the agreed service.

A **legal obligation** can also provide the basis for processing personal data. This may be an obligation under European or national legislation that requires companies to disclose information to the government. This is the case for companies including banks, insurers and airlines.

The **public interest** can also provide a legal basis, for example if the government agrees organisational arrangements with companies for tax administration purposes. This legal basis also allows the collection of data for scientific or historical research purposes. The tasks of the public authorities are also covered by the public interest.

[14] Article 6 : Recital 40-50

Moreover, the law provides that you may use the personal data of a data subject or another natural person **in matters concerning vital interests** (i.e. literally a matter of life or death). In that case, you must act in the interests of an individual person with sufficient common sense.

The last legal basis is **the legitimate interest of the controller or a third party**. This is not applicable to public authorities. If you rely on this legal basis, you must always make this clear and you must always weigh your interests carefully against the data subjects' right to privacy.

This must be clearly explained and demonstrated in your own records and in the privacy statements you draw up by way of explanations for the data subjects. A purely economic interest is no longer an adequate justification, and the processing operation must be necessary. It should be noted that this legal basis is the weakest.

The GDPR specifically demands that additional attention be paid to the processing of data about children (up to the age of 16). This requires the consent of the parents, which is not so easy to arrange.

Even stricter rules apply to the processing of special categories[15] of personal data. The processing of this kind of data is prohibited except in specific cases, which are set out in the GDPR.

These specific cases can be summarised as follows:

- If the data subjects have explicitly given their consent
- If the data concerned are already publicly available as they have been manifestly made public by the relevant data subject
- If this is done under employment legislation (all kinds of data need to be processed in connection with social security, legal requirements and contractual agreements)
- If a vital interest is involved and the data subject is unable to give consent (this often specifically concerns the use or transfer of medical data)

[15] Article 9 : Recital 51-56

- If processing is carried out for non-profit associations and charitable organisations, to the extent that the processing concerns the lawful use of data about members, former members or persons with whom the relevant association or organisation is in regular contact
- If processing is carried out for foundations, trade unions or political or religious organisations (with political, philosophical or religious aims)
- In the case of data concerning offences or criminal matters, data may be processed only by public authorities or in those cases provided for by law (EU or national). Each country may impose its own limitations. Criminal law is a national matter and is not laid down in the GDPR.
- If the data are required as part of legal proceedings
- In a number of cases where this is necessary for reasons of public interest:

    - in the event of a substantial public interest, and when covered by EU or national legislation that also protects the rights of the individual
    - in the context of healthcare (medical diagnosis; data for the organisation of health or social care systems and services; assessments of the health of employees; testing of medicines)
    - in the event that the data are required for scientific or historical research purposes or archiving purposes, in which case you need to take the necessary protective measures (research results can be anonymised or pseudonymised, for instance).

In every case, important grounds for processing personal data are always required. The legal grounds provided by the data subject's consent and the legitimate interest of the controller will be discussed in detail in the next chapters of this book.

4.2 Consent provided by data subjects

Obtaining consent[16] from data subjects provides the best legal basis for processing personal data. In practice, however, obtaining consent is by no means straightforward. Moreover, because the consent can be withdrawn at any time, this legal basis also entails an element of uncertainty.

[16] Article 4.11; Article 7-8 : Recital 32-33,38,42-43

Consent has played a part in privacy legislation for a long time, although the rules have become stricter over the years. At first, it was permissible to extract some kind of tacit consent, often as part of a more comprehensive contract and without a predetermined purpose. Later, allowing data subjects to withdraw consent (i.e. opt out) was made compulsory. Today, the GDPR imposes a whole string of conditions that need to be fulfilled in order for consent to be considered valid (opting in). Consent must be given voluntarily by an affirmative act, be informed, and be clear and specific, and must be able to be withdrawn just as easily as it is given.

Voluntary

Consent provided by a data subject cannot be used as a legal basis if there is an imbalance in the relationship between the controller and the data subject. This applies in the case of the relationship between an employee and an employer, for example, because the employee is not usually in a position to refuse consent.

In addition, consent may not be linked to the provision of a service unless the data are required directly for the fulfilment of the contract.

In that case, however, contractual necessity provides the legal basis, and so, for the sake of clarity, it is best not to request consent. In addition, consent for the use of data in subsequent marketing and advertising campaigns may not form part of any contract that is to be concluded or any general terms and conditions. Such consent is only valid under the GDPR if it can be provided separately from the conclusion of the contract.

Affirmative

Data subjects must make a clear statement themselves or perform an affirmative act to indicate their consent for a specified processing operation. Any suitable approach or method may be used for this purpose. The GDPR summarises the most common methods, which are giving consent by means of an oral or written statement, ticking a box, and activating a setting in a browser or an app. A new development in this area of consent is that the GDPR explicitly specifies that silence and inactivity cannot constitute consent. Pre-ticked boxes, for example, are absolutely forbidden. Failure to make use of an opt-out function or unsubscribe button does not constitute valid consent either.

This is an extremely important condition for all organisations that set up direct marketing campaigns.

Informed

Before you ask data subjects for their consent, they must be provided with detailed information about the identity of the controller, the planned processing operations, the purpose and legal basis, and the measures taken to protect their data. This must be done in an honest way, using clear and plain language. The purpose, the precise data that is required for that purpose, and the consent that is to be provided must all be clearly aligned. A detailed, comprehensive privacy statement is a suitable document for such communication. The information that needs to be included in the privacy statement and the best way to make it available to data subjects will be covered in a future chapter of this book.

Specific and unambiguous

Consent for the processing of personal data is always given for a clear purpose. The controller therefore cannot use the data for any other purpose unless the new purpose very closely resembles the original one.

A good example of such a purpose is contacting former or existing clients to inform them about a product or service that is closely related to a product or service they have already purchased.

You need to pay particular attention if you are considering combining data in a different way or using data for a completely different purpose. Data mining is problematic in this context. This technology is often used, for marketing purposes among other things, in order to discover potential patterns or unexpected associations in vast amounts of information, and so there is no predetermined purpose. The GDPR provides some room for flexibility in cases where data are reused, and the data subjects' explicit consent can be requested the next time the data are used.

Consent can be withdrawn

In every case, data subjects must be informed that they can withdraw their consent at any time. The procedure for withdrawing consent must be as simple as the procedure for providing consent. Under the GDPR, the controller is now specifically required to arrange this.

While this approach is fair and logical, putting this obligation into practical effect is not always straightforward, not least because the GDPR requires that the controller can clearly demonstrate the data subjects did in fact give their consent.

4.3 Consent or legitimate interest

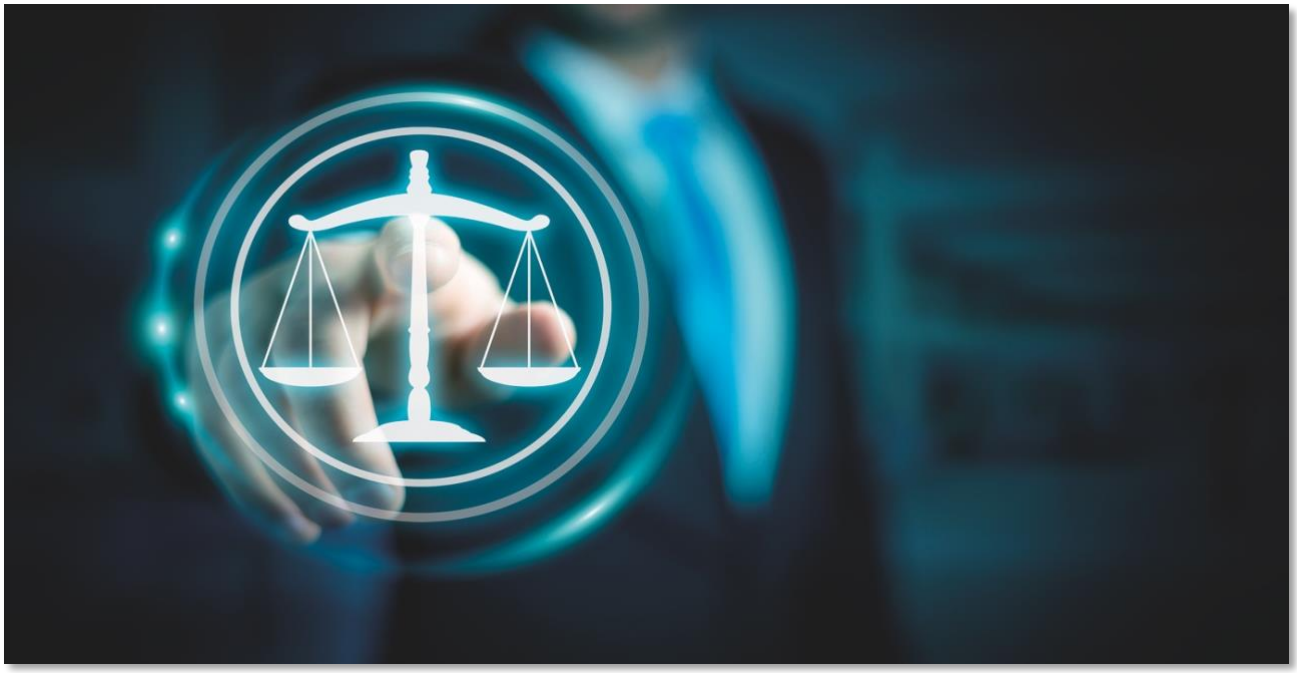
In previous chapters of this book, we looked at the different possible legal bases that exist for processing personal data. In some cases, there are a number of legal bases[17] that can be relied on. But how do you choose the best legal basis to justify your processing operations?

Answering this question is more difficult than it may seem. Nevertheless, it is important to take time to consider this aspect because the choice you make has consequences. Some legal bases provide more certainty in the long term than others.

Switching between different possible legal bases, however, causes confusion and can create the impression that you are trying to mislead the data subjects.

[17] Article 6-9 : Recital 47-49

The choice of legal basis is clear as long as the data in question is processed for the purpose of providing agreed services under a contract (e.g. contact details for orders, deliveries or the provision of services, and billing) or in connection with legal obligations. Choosing between obtaining consent from data subjects and relying on a legitimate interest, however, is much more difficult.



Requesting the consent of the data subjects always seems to be a good option but it also entails risk. If you request consent but fail to obtain it, this obviously means you are no longer allowed to process the relevant data. Imagine that you are planning a marketing campaign and you send a letter or e-mail to everyone listed in a file in order to request explicit consent to contact them in the future. As the response rate to this kind of communication is perhaps around 10%, the result would be that you would no longer be able to use the vast majority of your contacts.

You would, of course, be on safe ground in those cases where you could demonstrate you had obtained such consent. Obtaining consent would also allow you to create a positive image, by openly communicating your intentions and taking account of the preferences of your contacts. At the same time, however, it would make it difficult to disseminate your campaigns widely, and it would make it extremely hard to add any new recipients. Finally, there would always be a risk that at some point in time data subjects might go back on their decision and withdraw their consent, leading to a further erosion of your contact base.

In that case, what are the alternatives? You can always rely on the legitimate interest of your organisation as a legal basis.

To continue with the example of a marketing campaign, a commercial organisation cannot function if it does not have the chance to present and advertise its products. As mentioned previously, you have to put your case together carefully.

First of all, the data to be used for processing must be limited to data that is strictly necessary. Having less information automatically reduces the risk of a serious breach of privacy. A file that only contains contact details is obviously not as critical as a large data set that includes sensitive data.

Next, you need to take all measures necessary to properly protect the data and guarantee confidentiality. You have to demonstrate that the collected data cannot be used for another purpose.

This will allow you to maintain a balance between the interests of the data subjects and those of your own organisation. It is best to keep brief notes (or more detailed notes, if appropriate) of the line of reasoning you followed in your records. In that case, if any disputes arise later on, you will always be able to demonstrate that you have been acting in good faith and have considered the right matters.

Unfortunately, even if you take all these measures you cannot rule out the possibility that a legitimate interest which is used as a legal basis may be challenged at any time. A data subject who feels they have been unfairly treated or a competitor that thinks you follow unfair practices may submit a complaint to the Privacy Commission, which may lead to an investigation and possibly legal action.

The outcome of any such legal action will depend on how the auditors or court interpret the specific facts, and this may, of course, be different from your own assessment. In that case, you may be fined or prohibited from processing data, and you may have to pay damages. When giving its judgment and deciding on the remedial action to be taken, the Privacy Commission will take the overall situation into consideration. The facts will weigh more heavily in the case of an organisation that has failed to implement any aspects of the privacy legislation properly. If, however, you have taken the necessary measures and can put forward clear arguments as to why you believe certain processing operations are justified, the facts will not count as strongly against you.

We realise that this is not a clear answer and we have not provided a straightforward guideline, but privacy is a right that needs to be weighed against other rights and it will always be a matter of interpretation and debate.

That said, common sense and an honest, open approach go a long way. The next thing you need to do is clearly communicate and properly document the perspective you have adopted. And it goes without saying that you need to take the expected security measures throughout the data processing process in order to limit the risk of data breaches.

5. Transparency

5.1. What is a privacy statement and what should it contain?

In the previous chapters of this book we took a detailed look at the records of data processing operations. You need to keep records of the personal data that are processed by your organisation, the purpose for which these data are processed and the legal basis for these processing operations. Every organisation is required to keep such records since 25 May 2018. These records can prove very useful in many other ways. They form the perfect starting point for performing a risk assessment and for producing an overview of your organisation's data protection measures and internal procedures. We will consider this in more detail in future chapters of this book. In addition, well-kept records provide you with the input you need in order to inform data subjects about the processing of their data, which is the topic of this chapter.

The GDPR requires that you give transparent information to all data subjects, in other words every person whose data you use. Data subjects have the right to be aware of the processing operations in which their data are used. The text in which an organisation publishes this information is known as a privacy statement[18].

The GDPR lays down rules on the information that must be supplied to the data subject. Each of these items must be covered in the privacy statement.

- The **data controller** must identify itself by supplying the official name of the company or organisation in question and the full address of its registered office. If the organisation has appointed a Data Protection Officer (DPO), the privacy statement must also provide information on how to contact this person. An address, telephone number or e-mail address where the DPO can be reached must be provided as a minimum, but it is not necessary to provide his or her name. Organisations that do not have a DPO must refer to a contact point.
- The most important part of the statement is **the list of the personal data processing operations** carried on by your organisation. The processing operations must be described in sufficient detail, with separate listings for each purpose. Each time, you must indicate the **purpose** for which specific data are collected, the **categories** of data you process, and the categories of persons involved, the **processing operations** that are carried on and the legal basis on which you rely in order to be able to process the data.

[18] Article 13-14 : Recital 60-62

When producing this list, you can, of course, draw on your internal records to ensure you do not leave anything out.

- You also need to be clear about the **recipients** of the information, in other words who will have access to it and who it will be passed on to. You should state which categories of your employees are involved in processing the data and are therefore able to access the information, and whether any external parties are involved in the data processing operations. If the collected information is passed on to third parties for further use, this must be indicated explicitly. This is normally done using general wording such as 'sister companies' or 'partners'. The GDPR expects you to be as transparent as possible, since it is important that the data subjects understand where their data ends up, although you obviously cannot be expected to list the full names of each of your partners or suppliers.
- You must demonstrate that **adequate security measures** have been taken to guarantee the confidentiality and integrity of the data. Once again, you do not have to go into detail about all the technologies and procedures involved, as this would obviously undermine the security measures, but you should disclose the principles you followed and how you are able to safeguard them within your company or organisation.
- You are specifically required to provide information about **the retention time (length of time data are kept)**. The GDPR states that you may use personal data for the intended purpose only, and you may therefore not keep data any longer than is necessary for that purpose. Moreover, as a data controller you have to guarantee the quality of the data. This includes guaranteeing that the data are not obsolete. Information about the retention time should be provided separately for each purpose.
- Moreover, the privacy statement must also clearly set out the **rights of data subjects**.
    - They may submit a complaint to the Privacy Commission at any time if they believe data are being processed wrongfully.
    - They may ask the controller to supply information about the processing operations that use their data, and you must explain how to do this.
    - They may inspect the information available on them personally and arrange for it to be changed or erased if they so wish.

The rights of data subjects will be the subject of a separate chapter of this book.

- Finally, the GDPR demands that you specify whether you transfer certain **data outside the EEA**. In that case, additional risks exist in relation to data protection and the rights of data subjects. These risks include the powers held by foreign authorities, such as NSA in the United States. Other guarantees apply, depending on the country to which the data are exported or the sector in which the company or organisation is active.
- This is a very complex subject from a legal perspective. In most cases, all you will need to state is that the data will remain within the EU and will therefore continue to enjoy the full legal protection provided by the GDPR. If that is not the case, you have to specify where the data will be sent and the form of protection that will apply. Data subjects can then decide for themselves whether their data will remain sufficiently confidential.

Besides specifying what the privacy statement must contain, the GDPR also provides guidelines for its design and structure. Important aspects include the way in which information is communicated to data subjects, when you present this information and how you keep it updated. These aspects will be considered in the next chapter of this book.

5.2. What is the best way to present a privacy statement?

In the previous chapter of this book we went over the different matters that need to be included in a privacy statement to ensure that all data subjects have been correctly informed about the processing operations carried on with their data. The way in which this is done is also important, and the GDPR drafters paid specific attention to this matter.

As a data controller, your duty is to provide this information **in a concise form and in clear and plain language**[19]. Some companies have excelled at producing convoluted texts, often dozens of pages in length, containing formulations that are incomprehensible to the layman, which deters users from actually reading the document and is the antithesis of transparency. The GDPR expects you to use simple language that can be understood by just about everyone. In the Netherlands, CEFR language level B1 is specifically recommended, which is equivalent to primary school level. If your audience includes any children, it is particularly important that you explain in a simple, intelligible way what you do with the data they supply. Drawing up a separate privacy statement for children is often the best solution.

Transparency can also be enhanced by providing an outline of **the main elements first** and by ensuring the text has a good structure. For example, you can describe each topic in one sentence or a brief paragraph, and then give visitors **the option to click** for further information. In this way, users can quickly find the items they are looking for and learn more if they so wish. It can be a good idea to use icons so that the message can be communicated more simply than with words alone. There are working groups that have been working on developing specific icons for years, but this task is proving a challenge.

Do not forget to place the **date and version number** on your privacy statement. Texts of this kind are not set in stone, since the nature of the data you process, the recipients or the protection measures taken may change. Your text must provide accurate, up-to-date information and will therefore be changed frequently. You are also supposed to keep data subjects informed about such changes. At the very least, you need to make clear to them that the privacy statement may change in future. Ask them to visit the page on your website regularly. It is worth keeping the old versions of your privacy statement so that if a processing operation is challenged you can check which information was available to data subjects at the time the relevant processing operation was carried out.

[19] Article 12.1 : Recital 58

The form your privacy statement should take and the best place to publish it depend on the circumstances. You need to ensure that it **is easy to find**.

You should avoid hiding your privacy statement among your general terms and conditions. While the most common method is to provide a link on the website, a privacy statement can also be communicated on paper or even orally. There are, however, a number of rules you need to take into account.

If you allow users to enter personal data on a website or in an application, you have to ensure the required information about data processing is provided **first**. The best way to do this is to refer to the privacy statement in the introduction to the application in question. Many websites do this in a bar at the bottom of each page. This is, of course, not very specific and does not relate to a single specific purpose, but it does ensure the information is made accessible to visitors as soon as they enter your website. This is important for websites that use cookies or other tools to collect information about the surfing behaviour of visitors. As they start working as soon as the website is entered, visitors must be notified immediately.

There is certainly nothing wrong with making **several privacy statements** that are adapted to different target groups. Your existing or prospective clients are probably not interested in how your organisation deals with staff data, and so using different privacy statements allows you to adjust the length of the text.

Tip:

As it is, the GDPR provides an excellent opportunity for every organisation to examine their **policy on processing staff data** and report on this internally. The volume of data about staff in circulation is greater than you would imagine and includes sensitive data.

- Payroll processing requires all kinds of data (salary, attendance, sick leave and composition of family). At many businesses, this information is processed externally by a social secretariat, which is therefore the processor of the data. Furthermore, data have to be passed on to the government for social security and tax administration purposes.

- In addition, the organisation's personnel files contain all kinds of career-related data. This information is also accessed by people outside the HR department in connection with recruitment activities, evaluations and promotions. It is important that you make any necessary improvements to the procedures surrounding confidentiality.
- Other data that are available relate to the use of IT tools. These can range from the content of e-mails to user accounts, user groups, authorisation levels and logs of the use of applications or visits to websites. It is important that you provide transparent information about the data recorded in the logs and the related purpose. You also need to make clear what the employer may and may not do with this information.

Larger organisations have to discuss this subject with the Works Council. Employees at smaller companies also need to be informed about all processing operations using personal data. This can be done in the form of an internal privacy statement, which you can include in your employment terms and conditions, or alternatively distribute as a separate document, either on paper or in a digital format. It is not a bad idea to ask your employees to sign this text to indicate they have read it.

While more creativity may sometimes be required, every organisation can, with a few efforts, shed light on the personal data processing operations it carries on and why they are necessary, as transparency is a basic requirement. Our next chapters of this book will consider what the GDPR means by adequate measures to protect personal data that are processed. This could present a major challenge for many companies.

6. Security for personal data

6.1. Adequate security for personal data

So far, we have mostly looked at the GDPR guidelines for the actual processing of personal data, including the conditions under which you may process data and how to communicate properly with data subjects. In addition to this, the GDPR requires that you adequately protect the data against risks during processing and at all other times.

While earlier legislation already included an information security obligation[20], under the GDPR responsibility for information security, which used to be restricted to the controller, will also lie with every processor that handles personal data on the instructions of a controller.

In order to explain how you can comply with this obligation, we first need to consider what information security involves. Obviously, larger organisations and also companies that handle confidential data on behalf of their customers on a systematic basis, have plenty of experience in this area. There are many different standards for information security, of which the best known is ISO 27001, and a vast array of policy papers, procedures and operational instructions exist to help organisations and their management, which can be considered a 'science' in itself.

[20] Article 24.2 en 25; Article 32

An information security program helps you to take the necessary steps in a systematic manner. You need to be aware of the specific risks to which the data are exposed and try to remove or limit these risks or reduce their impact.

The GDPR does not specify exactly which measures are required to ensure adequate security. This is because the appropriate approach depends on many aspects.

On the one hand, the risks are not always the same:

- The impact of any data breach is determined by both the quantity of the data and their nature (special categories, sensitive data or identification data as opposed to quasi-public data).
- The nature of the processing operation itself may entail specific risks. For example, additional attention has to be paid to automatic data analyses that are used as a basis for decision-making.
- Exchanging or transferring data may create extra risks.
- The involvement of third parties in the processing operation may pose an additional threat.
- The same protection does not apply outside Europe (more specifically outside the EEA).
- The length of time for which data are kept can also play a role.

On the other hand, science and technology are not standing still. This means that what counts as adequate security today may no longer be considered adequate in two years' time.

It therefore comes down to striking a balance. The costs and effort involved in taking specific measures must be proportionate to the nature of the data and the damage that could result if something goes wrong.

Larger organisations undoubtedly already apply a great many procedures. They formulate their policy on information security and have a management system in place, they identify the risks and consider whether they are acceptable, they draw up procedures and instructions, they perform checks and arrange for external audits to be carried out, and they analyse incidents and learn from how procedures work today so they can make improvements moving forward. All of these steps are incorporated in the standards of ISO 27001, for example.

Let's consider the basic principles.

In the first place, you need to identify the threats to which personal data (just as all other confidential data) are exposed and from which they require protection. Many people refer in this context to the CIA principles (any resemblance to a well-known US organisation is purely coincidental). In this case, CIA stands for confidentiality, integrity and availability. Information security guarantees the confidentiality, integrity and availability of data.

- Guaranteeing **confidentiality** means ensuring that data are not made public and do not end up in the hands of anyone except the intended recipient. We are all aware of notable examples of the theft of hundreds of thousands of credit card details or the publication of confidential documents by hackers.

Data breaches can, however, take much smaller forms, such as a letter that ends up in the wrong letterbox or an e-mail that is sent to the wrong recipient, either deliberately or accidentally.

- Protecting the **integrity** of data means that no data may be wrongly changed or erased. Falsification may be a straightforward case of fraud. Hackers are able to manipulate data, but unintended changes are much more frequently the result of human errors made when writing software or configuring systems or applications.
- Finally, you need to guarantee the **availability** of the data. Measures such as backups or a disaster recovery plan are designed to ensure that data are not lost and can be viewed and processed when required.

If you already have a management system of this kind in operation, you will not need to take much additional action to ensure your information security is ready for the GDPR. Obviously, you need to ensure that all personal data are classified as confidential and that the procedures for handling confidential data are applicable to them. Some additional procedures will probably also be required to improve the arrangements for specific personal data processing operations. Apart from that, however, the general framework will be applicable.

Firms or organisations that are not well versed in information security face a much greater challenge. In the next chapters of this book I will therefore provide tips on dealing with information security at small organisations, including how to minimise the risk of incidents involving personal data by developing practical procedures and implementing measures in a pragmatic way using common sense, and how to demonstrate that you have done this in an adequate manner.

6.2. Personal data risk assessment

The GDPR places a great deal of emphasis on the fact that all controllers and processors of personal data must adequately protect the confidentiality, integrity and availability of the personal data. Even if you do not have any specialised staff to take care of this obligation, it is perfectly possible to comply with it by taking a simplified approach.

The starting point for all measures is a risk assessment[21]. Although this sounds difficult and serious, it does not need to be complicated. Simply take your records of data processing operations and go over them, step by step, and ask yourself a few targeted questions.

Next, add two more columns to your records. In these columns, specify the risks associated with each specific processing operation and the measures you can take to limit these risks.

I'll give some simple examples that you are also likely to find in your own records. You will have a data set containing the contact details of people to whom you like to send information about your products and services every so often. You obviously hold data about their name and address, and also about the business they work for, their positions and perhaps their studies, hobbies and areas of interest, too. Besides this, you will have all kinds of data relating to your own employees. You keep updated information about their career development and annual evaluations. Every month, you provide the social secretariat with details of employees who were on leave or were sick. You have to know the make-up of their families, because this needs to be taken into consideration when calculating payroll tax. And perhaps your security cameras film everyone entering and leaving your premises.

There are plenty of other examples, and it is impossible to conceive of any situations in which no personal data are processed at all.

What are the risks that exist with regard to the security of this information? A great deal depends on how you store the data, in other words the technology you use.

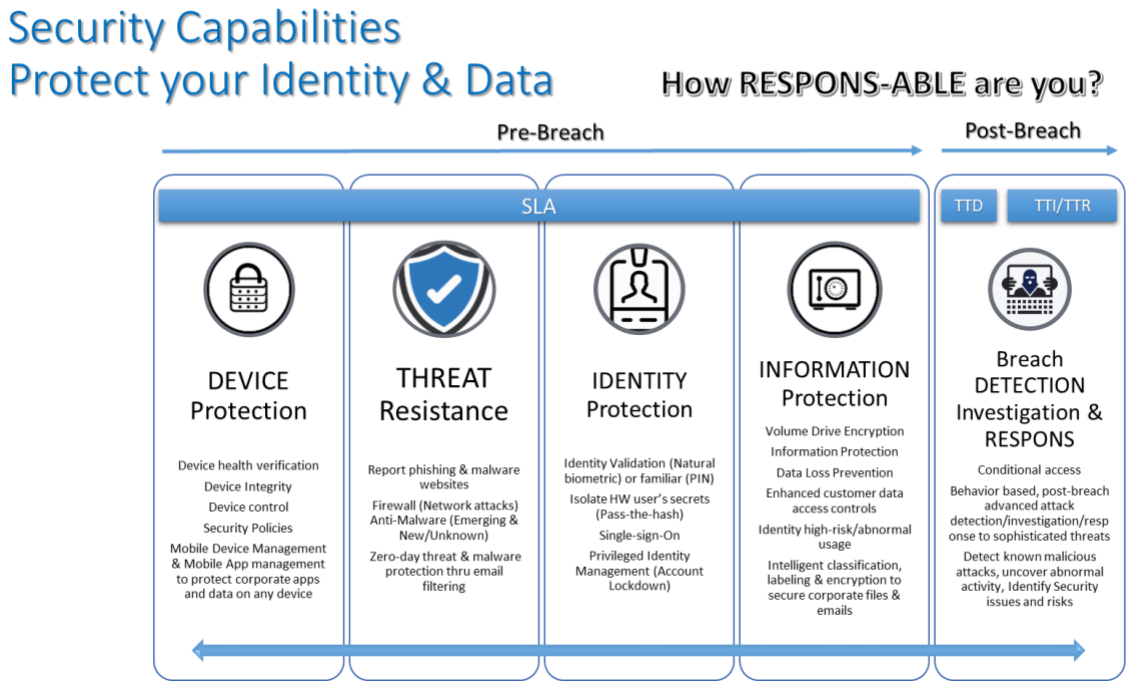
- If you work with paper files, it is important to consider whether folders and index card holders are openly accessible on your desk or are locked away in a cupboard. In the latter case, you need to identify who has access to your office and who can get their hands on the key. Do you close the door when you leave? Do you put the papers away?
- In the case of files stored on a computer, essentially the same questions apply, although the answers will be slightly more complex. Perhaps you work offline on a laptop computer. Does this computer have a password? Are you the only person who knows this password? Are the confidential personal data contained in a file that has password protection? When you take your laptop computer out of the business's premises, does it have any additional protection? Do you sometimes leave it in your car? Where do you keep it in your home?

[21] Article 32; Article 35-36 : Recital 75-76, 84, 89-95

- The situation is different again if the data are stored on a server rather than locally. Do all users of the server have access to all data? Do they actually require this? Are you able to split the server into zones and assign different levels of authorisation to different users or groups? Is the server backed up, and where are the backups kept? Is there an IT company that carries out maintenance work on the server park? Does it have access to all data? Have you reached agreement with the company on what its employees can and cannot do, despite the fact they effectively have full rights (which they require to perform their work)?
- Are the data stored in the cloud? In that case, where are the data actually located, and who has access to the data? What guarantees has the cloud provider given? Are any data transferred abroad or even outside Europe, where they are not protected by the GDPR? Are the data transferred in a secure manner?
- Are the security camera images saved and stored? How long do you keep them? Who is able to view the data, and in which circumstances are they actually consulted?

As you may have gathered from the above questions, by taking measures in each of these situations you can dramatically reduce the risk of violations and infringements. The examples also show that the risks differ, depending on the precise contents of the files. If a file contains contact details only, a breach of confidentiality will not have a huge impact. This is not the case, however, where certain types of personal data are concerned.

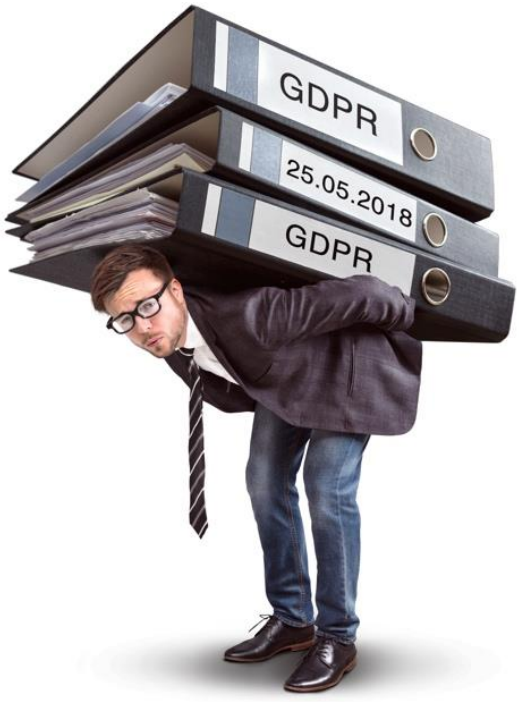
Much stricter security is required if, say, you work in the healthcare sector and keep records of sensitive data relating to patients or clients (which amount to medical data) precisely because a breach of confidentiality or integrity can have much more serious consequences. Depending on the size of the database, the impact may become greater as the number of data subjects increases. The measures that you take in relation to each of the listed risks must always be commensurate with the assessment of the risk.



Given this, it is logical that the GDPR imposes greater obligations on all organisations that use special categories of personal data and on all organisations that systematically process personal data as their core activity. In some cases, a formal data protection impact assessment (DPIA) has to be drawn up and submitted to the Data Protection Authority before processing takes place.

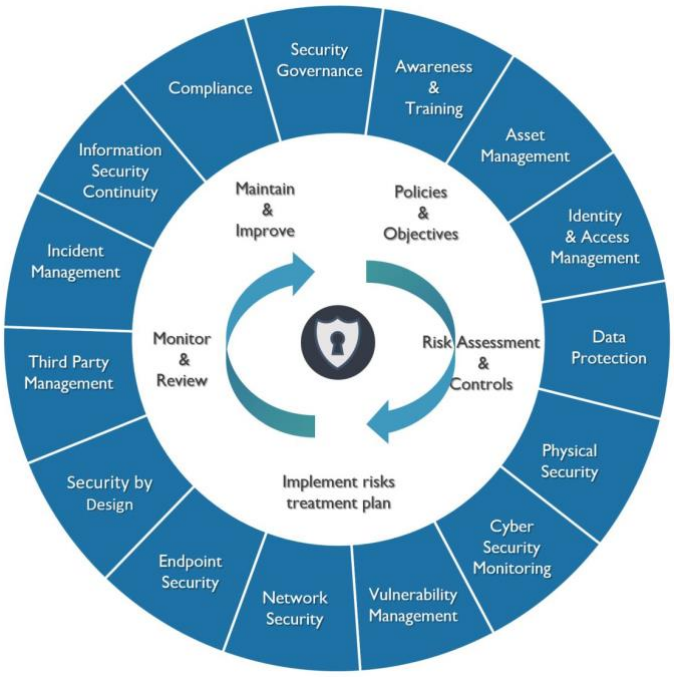
It is advisable that all companies and organisations perform largely the same exercise. Keeping proper notes and records of the findings is also recommended, so you can demonstrate at any time that you handle personal data legally and with respect. Specialised software or methodologies can be useful, but in many cases they are unnecessary. The two columns mentioned above, which you can link to simple records of data processing operations, will supply much of the evidence you will require, provided the information is entered with due care.

In the next chapter of this book we will take a closer look at the areas in which protection measures can be implemented to ensure personal data are stored and processed securely.



6.3. Measures to protect personal data

In the previous chapter of this book, we discussed the importance of an impact assessment. The size of each risk determines which protection measures[22] are needed. In this chapter we discuss the actual measures to be taken. Obviously, a small organisation will not tackle matters in the same way as a large company. That said, a brief introduction to the framework of a system such as ISO 27001 is useful since you need to follow the same reasoning and logic.



The first aspects covered by ISO 27001 relate to **policy and organisation**. You need to formulate the starting points of your policy. This can be done in as little as two sentences. The use of personal data must be legal and have a legitimate purpose. You must also ensure the data are adequately protected. The general manager is responsible for shaping policy in this area. Although the general manager may delegate this task, he or she remains responsible and must also assess the policy's effectiveness every year.

The division of tasks in this framework of data protection within but also outside your organization will add an extra layer of corresponding responsibilities. Therefore, it is recommended to establish a core team, because the manager can't do this all by himself keeping track of all duties and tasks that needs to be done.

[22] Article 32 : Recital 77-78

He will then be able to focus controlling the core team, who will be responsible to make an inventory as accurate as possible off all information carriers which will be updated and, where necessary, adjusted in function of the use. With this inventory one can start with a risk analysis which will later be used to provide the necessary ' controls ' to reduce the risk of data loss.

The next aspects relate to **measures in various areas** that need to be taken in one way or another by all businesses and organisations, regardless of their type.

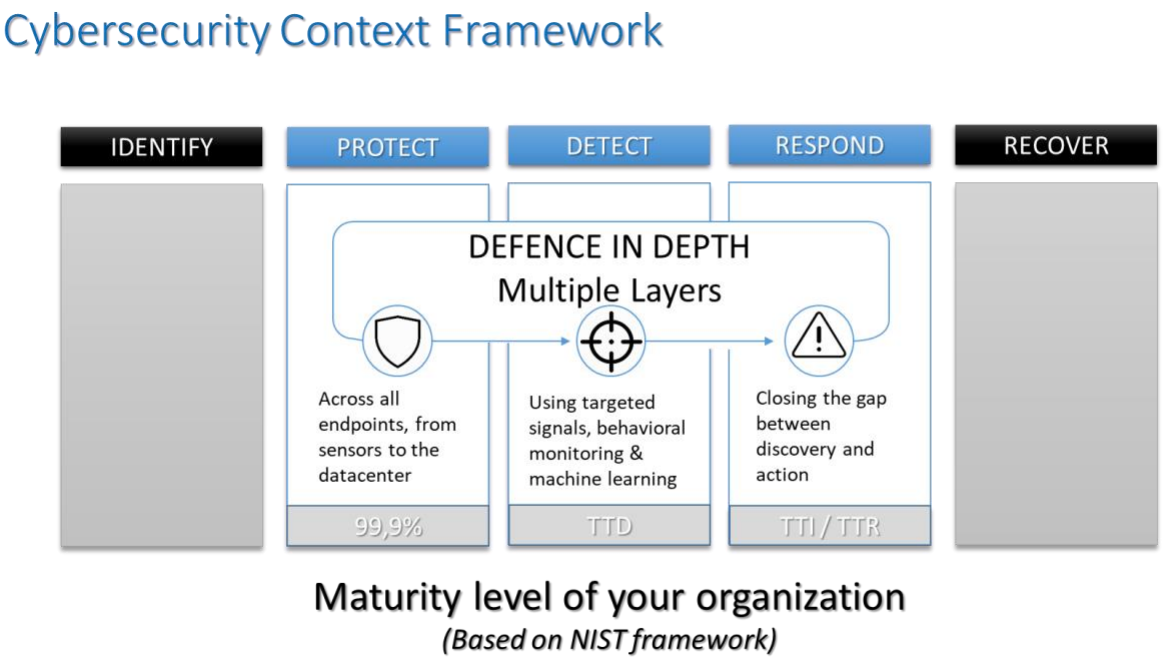
- Employees (screening / training and awareness / former employees)
    - When recruiting employees, pay attention to the candidates' sense of responsibility.
    - If you process sensitive data, ask for a list of previous convictions (you will also have to treat this as sensitive information!).
    - Include a confidentiality clause in your employment contracts. This may take the form of a simple sentence, such as: 'All personal data that you use in your working environment are confidential and may be used only for the task you have to perform.'
    - Ensure your employees (and you) are given training relating to data protection on a regular basis.
    - Make sure that former employees no longer have access to data and do not hold on to any business assets (including data on paper or in a digital format).
- Classification and use of assets
    - Keep records of data processing operations and supplement these records by performing a risk assessment.
    - Take care with removable media (e.g. memory sticks containing data) and devices that are to be scrapped. Take steps to prevent data from falling into the wrong hands.
- Access rights
    - Ensure that your passwords are sufficiently complex and keep them strictly private.
    - Allow your employees to access only the information they require to perform their work. Use job categories for this purpose.
    - Restrict administrator rights in systems to authorised persons only.
- Cryptography
    - The GDPR specifically mentions data encryption as a protection measure, and it is certainly advisable to use encryption when exchanging data or storing it for long periods of time.
    - Examples include the use of the HTTPS protocol on websites, the SFTP protocol for data transfers, and e-mail encryption.

    - An IT partner may provide assistance. Do not forget to reach proper agreements with your IT partner so that it does not present a new security risk.
- Physical security
    - Turn on your PC's screensaver when you are not at your desk.
    - Do not leave any documents lying around at the end of the working day (clean desk policy).
    - Develop a key plan for desks and cupboards.
    - You might require gates, an alarm system, camera surveillance or a badge system, and perhaps separate zones within your buildings.
    - Protect your equipment against power cuts. Take steps to prevent mechanical failures.
    - Always accompany visitors and provide them with confidentiality guidelines.
    - Pay additional attention to rooms containing sensitive data, such as server rooms or archives where confidential dossiers are stored.
- Network security
    - Use a firewall, virus protection and content filtering to protect your network against external risks.
    - Divide larger networks into zones. Take steps to prevent system failures. Monitor and log network activity.
- Security measures to be taken when developing applications or systems
    - Separate the test environment from production and develop rules for transferring data.
    - Always consider security and perform tests before bringing systems into use.
- Monitoring processing operations by third parties
    - Reach contractual agreements on security and data protection with your suppliers.
    - Assess the operations of your suppliers and follow up your assessments on a regular basis.
- Continuity
    - Ensure proper maintenance and deduplication to reduce the risk of system failures.
    - Back up data and draw up a system recovery plan for use when serious problems arise.

- Incident management
    - Record all incidents that expose you to the risk of data privacy violations.
    - Any data breaches that may have an impact must be reported.
- Audits
    - Check your security is adequate and have it evaluated.

Although the measures in this list are obviously examples, and every organisation will handle implementation in a slightly different way, you can use the list to help you identify all the areas in which you can actively reduce risks.

We will take a closer look at some of these areas, to which the GDPR pays special attention, in the upcoming chapters of this book. These include monitoring subcontractors and other third parties, and what you need to do in the event of a data breach.



6.4. Managing risks associated with subcontractors & data processing agreements

As we noted previously in this book, risks can arise, and therefore security measures need to be taken, when companies and organisations engage subcontractors[23].

The GDPR is very clear on this point.

Although subcontractors have their own responsibilities and a number of obligations, a data controller that engages a subcontractor in the role of processor always remains responsible for the data.

The controller must select each subcontractor carefully and guarantee the performance of the contract, it must clearly formulate and define the relevant task, and it must verify that the subcontractor complies with its instructions and the legislation, particular with respect to security.

In recent years there has been a growing awareness among information security specialists that subcontractors always pose a risk. It is therefore unsurprising that the GDPR pays plenty of attention to this issue.

Various steps need to be taken in the different phases of a working relationship.

When **selecting suppliers**, attention must always be paid to data protection and information security. The controller must make sure that any subcontractor it intends to engage is aware of its obligations and can fulfil them adequately. There is no system of certification to prove a company is 'GDPR compliant', and I have not heard of any specific plans to introduce such a system.

That said, the official bodies are encouraging professional associations to draw up codes of conduct that people can sign to show they know the rules and are prepared to follow them, and questionnaires are increasingly being used in selection procedures and in tender documentation. It is, of course, possible to obtain a certification in the area of information security, but the certification paths are highly geared towards large organisations and are not a viable proposition for every company or organisation. Always ask your future supplier about its information security policy and the applicable measures and include both aspects in your selection criteria. Finally, keep records of the documentation you have collected.

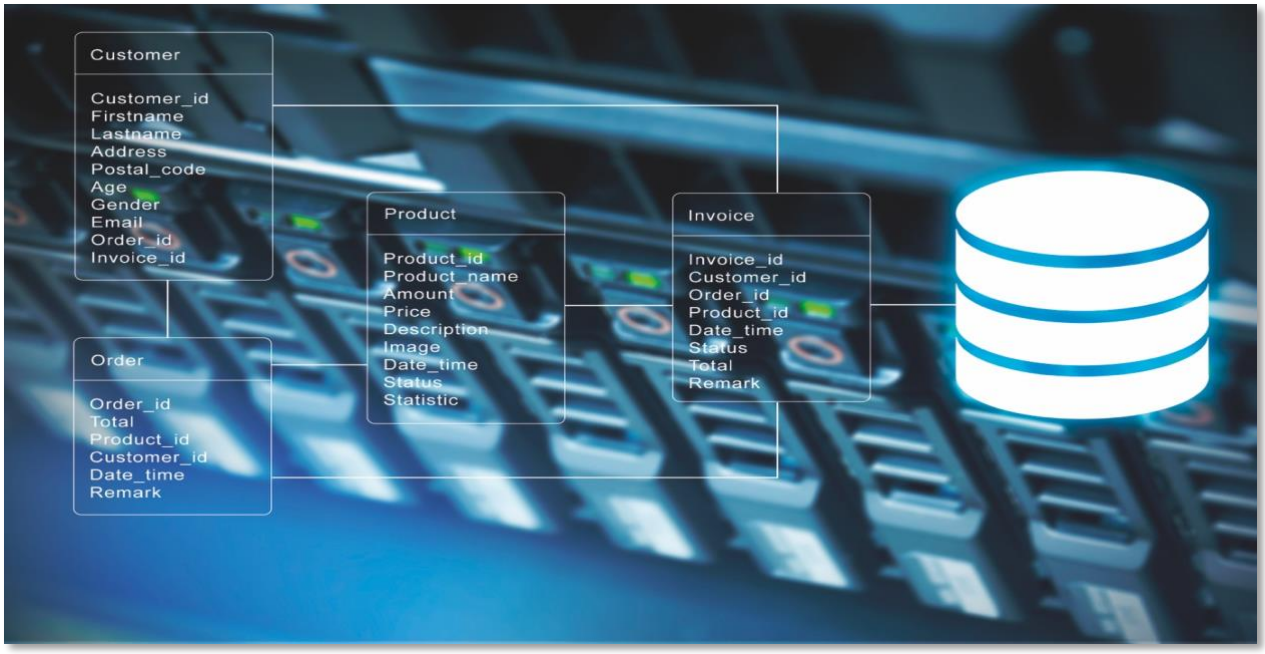
[23] Article 28-29 : Recital 79 en 81

When **assigning a task**, it is essential that you have some contractual clauses on data protection. The best way to do this is in the form of a data processing agreement. This may be an appendix to another contract or a framework agreement. Some general clauses can also be incorporated in your general terms and conditions, of course. Even if you have been working with a subcontractor for a long time, you still need to ensure that the subcontractor complies with the GDPR. Given the differences between the GDPR and the previous legislation, which placed less emphasis on the processor's obligations, it is advisable to draw up an amended version of your data processing agreement.

All such data processing agreements need to include the following clauses:

- The principal is assigned the role of controller, and the contractor/supplier/subcontractor is assigned the role of processor.
- The processor may use the data only in accordance with the controller's formal (preferably written) instructions.
- The processor respects the confidentiality of the data and also imposes this obligation on all its temporary and permanent staff.
- The processor must offer an adequate level of data protection and ensure that the data are, and remain, available for the task (using backups and measures to ensure continuity).
- The controller must be informed immediately in the event of a data breach, and there must be a procedure in place to limit the impact of the breach. No information may be provided to the Privacy Commission or data subjects by the processor itself.
- The processor must remove the data once the task (or the agreed retention period) has ended, and it must also be able to demonstrate that it has done so. Where applicable, it must also return the data to the controller.
- Data must not be passed on to third parties unless the controller has given its consent. If the processor engages a subcontractor with the controller's approval, it must ensure that the subcontractor accepts the same obligations as those set out in the data processing agreement.
- The processor permits the controller to monitor the proper performance of the contract by carrying out assessments or audits.

As a smaller organisation, you might be able to benefit from work done by your larger suppliers, which have probably already drafted their own standard processor contracts to present to their clients. At our company, we have taken steps to ensure that our customers do not have to go to great lengths themselves to find out what the rights and obligations of the controller (principal) and processor are.



We have attempted to draw up a balanced contract, which we presented to our customers.

Finally, the controller also has **to check whether the processor fulfils the contract properly**. In the case of longer-term contracts, it will have to verify whether this is the case on a regular basis. In connection with this, it is essential that the contractual agreements include the right to perform audits. Of course, this does not mean that controllers will have to audit all subcontractors every year themselves. Large organisations perform such audits – often much to the annoyance of their suppliers – at processors that they believe pose a high risk of a personal data breach or where a personal data breach would have a major impact. In many cases, it is sufficient to check whether the supplier's certification is renewed every year. Alternatively, you can ask the supplier to complete and sign a questionnaire in which the measures taken by the supplier have to be summed up.

As with all aspects of this legislation, the actions to be taken must be weighed against the likelihood of an incident occurring and the potential impact this would have.

7. Data Breaches

7.1. incident management

In the previous chapters of this book we explained how you can take appropriate measures to ensure the personal data that you process is properly protected. You need to understand the potential risks, you need to take various measures to reduce the risks or remove them if possible, and if you engage subcontractors you need to ensure that they organise matters as well as you do. However, things can still go wrong. This chapter looks at what you need to do in such situations.

A data breach[24] is a situation in which confidential data are lost, are wrongly changed, are made public, or fall into the wrong hands. The GDPR requires that the controller, who is responsible for the processing of personal data, must report any data breaches that could constitute an infringement of the privacy of data subjects without unnecessary delay to the data protection authority. If there is a serious risk of damage, the data subjects will also have to be informed.

[24] Article 4.12; Article 33-34 : Recital 75 en 87-88

Before considering whether a data breach has to be reported to the Data Protection Authority, I will first focus on incident management. After all, your primary obligation as a controller or processor of data is to prevent incidents and minimise the impact of any incidents that do occur.

First of all, you have **to spot incidents at the earliest possible stage**. There are many network tools that can reveal abnormal behaviour in the network, detect viruses or malware, or apply content filtering, which you can use for this purpose. That said, alert employees are also capable of spotting infringements. It is therefore crucial that staff training or awareness campaigns are organised on a regular basis, to ensure everyone is clear about what constitutes an abnormal or worrying situation. It is also important that all employees know who needs to be called upon when an incident occurs.

Second, you must take steps as soon as possible to **end the incident or limit its impact**. All employees have to comply with a number of rules. If they come across information in a place where it does not belong, they have to delete it or notify someone in charge. This information may be found on physical carriers or in files located in the network. If they encounter unescorted strangers in a secure zone, they have to raise the alarm, and so on. When monitoring alerts point to hacking or an infected system, system engineers will need to examine the system as soon as possible and may have to shut it down as a preventative measure.

In cases of doubt, it is best to stop processing operations and block transfers of processed data until it is certain that a problem exists and the degree to which the processed data have been affected is known. By doing this, you can often ensure an incident does not ultimately become a data breach. As long as wrongly processed data are not disseminated or disclosed, no infringement is deemed to have occurred, and hence there is no impact to deal with. In that case, strictly speaking there is no data breach.

Next, an **analysis** of the facts can be started, if necessary, in parallel with the above. This will establish the true **cause of the problem**. You can then think about making **improvements** to the organisation, systems, applications and the way employees work in order to prevent a reoccurrence.

The analysis will also consider **the potential or actual impact**, whether the confidentiality and integrity of the data is at risk, whether any of the data are personal data, and the possible consequences of the infringement. In many cases, establishing the amount of data, and therefore the number of people, affected by the incident will take some time. Moreover, whether an actual risk of an impact exists, and in particular the potential extent of the damage, is not always immediately clear.

You need to be able to answer the above questions before you can decide whether the data breach has to be **reported** to the Data Protection Authority or the data subjects. Whether you need to do this, and, if so, when, will be the subject of the next chapter of this book.

In addition, all incidents must be **logged in your internal records**. All incidents must be analysed - actual data breaches as well as near misses. The resulting information is crucial for evaluating the existing procedures and guidelines and for checking whether the measures taken provide adequate protection against the possible risks. The causes of an incident must be recorded, as must the planned remedial actions. Following up incidents according to a fixed plan will systematically improve your organisation's security.

In extreme cases, a data breach may have disastrous consequences. An organisation may be confronted with huge communication problems if highly sensitive information about a large number of data subjects is leaked. In some cases, the data breach is known to people outside the organisation and the press is already aware of it. In such situations, it is useful to be able to fall back on pre-prepared **crisis communication** scenarios. If your organisation has taken out cyber security insurance, your insurer might be able to help you with this.

Where there are suspicions that criminal offences have been committed, you must also ensure that a **legal file** is compiled swiftly. It is sometimes necessary to make a quick backup of the situation at the time the incident was discovered, or set aside log files, before the relevant data disappears or are changed by steps taken to resolve the incident. Obviously, this will sometimes mean going against what needs to be done to limit the existing problem quickly.

If the police or courts are involved, you must also never lose sight of what you can, and cannot, do when acting on your own authority, particularly if your role is that of processor. In that case, you need to involve the controller at the earliest possible stage. If the authorities require that you hand over information, you will still be under an obligation to the controller to protect this information insofar as possible, and you must ensure that you do not divulge any data (e.g. relating to other data subjects) that is not required for the purposes of the investigation.

These steps should be well-documented so that everyone within the organisation is aware of them and acts accordingly. It will also help you demonstrate that you take your obligations under the GDPR seriously.

7.2. Notification obligation

As we explained in the previous chapter of this book, once a data breach has been identified the first concern is to minimise the impact of that breach. In addition, the GDPR requires that the controller notifies[25] the Data Protection Authority without undue delay of each data breach that probably carries a risk of an infringement of privacy. The data subject will also have to be informed if this risk is likely to be serious.

This obligation raises a great many questions. When does an information security incident become an actual data breach? When does a data breach pose a risk of a privacy infringement? When is there a serious risk of damage? At which point do you become aware of the incident and have an obligation to report it?

If the incident involves personal data, you must in any event inform your data protection officer (DPO). If you do not have an official DPO, it is essential that someone assumes this role. The DPO is in the best position to determine the data's importance and how serious the potential impact of an infringement would be for the data subjects and for the controller (this is either your own organisation or, if you are a processor that is commissioned by another party, your client). The DPO advises the organisation about the communication that needs to take place. He or she is also the person who is best placed to decide whether the Data Protection Authority needs to be notified and which information can be provided directly.

Tip:

More simply, you can ask yourself three questions to determine whether notification is necessary:

1. Has there effectively been a data breach? If a situation had the potential to result in a data breach but no data were disclosed or fell into the wrong hands, it is not considered to go beyond an incident. You must therefore record it in your internal log, but notification is not necessary.

[25] Article 33 en 34 : Recital 85-88

2. Does the incident probably entail no risk? Even if data end up outside the secure zones or outside your organisation, it may still be the case that there is no actual risk owing to the protection measures that have been taken. For example, the data may have been encrypted in such a way that they cannot be used by outsiders.
3. Is there a serious immediate risk of damage to the data subjects? If there is a data breach involving credit card details, for instance, there is a risk of financial damage and the data subjects must be informed as soon as possible so that they can take steps themselves. This may also be the case if the data breach involves various kinds of sensitive information. If the data involved are trivial, informing everybody is a less urgent matter. The GDPR also provides for situations in which it is almost impossible to notify all data subjects individually. In such cases, public communications are also considered adequate.

The GDPR also lays down rules specifying the information that must be included in the notification:

- a description of the infringement, indicating the type of data subjects and the categories of data insofar as possible
- the approximate number of data subjects, where possible
- the contact details of your DPO or the contact point for data privacy matters
- The probable impact of the infringement
- The measures taken by the incident team to limit the impact

Some of this information may not be available immediately, and further analysis might be required to establish some of the facts. The GDPR therefore specifies that notification must take place 'without undue delay', and not 'immediately'. The standard is to notify the supervisory authority not later than 72 hours after the controller becomes aware of the data breach. Notification can also be delayed for more than 72 hours provided a reasonable explanation is given. Part of the information about the infringement may also be supplied later than the initial notification takes place.

If you act in the capacity of processor, and not that of controller, you must be particularly careful when a data breach occurs. This is because you run the risk of stepping outside the bounds of your own area of responsibility and becoming increasingly exposed to liability as a result.

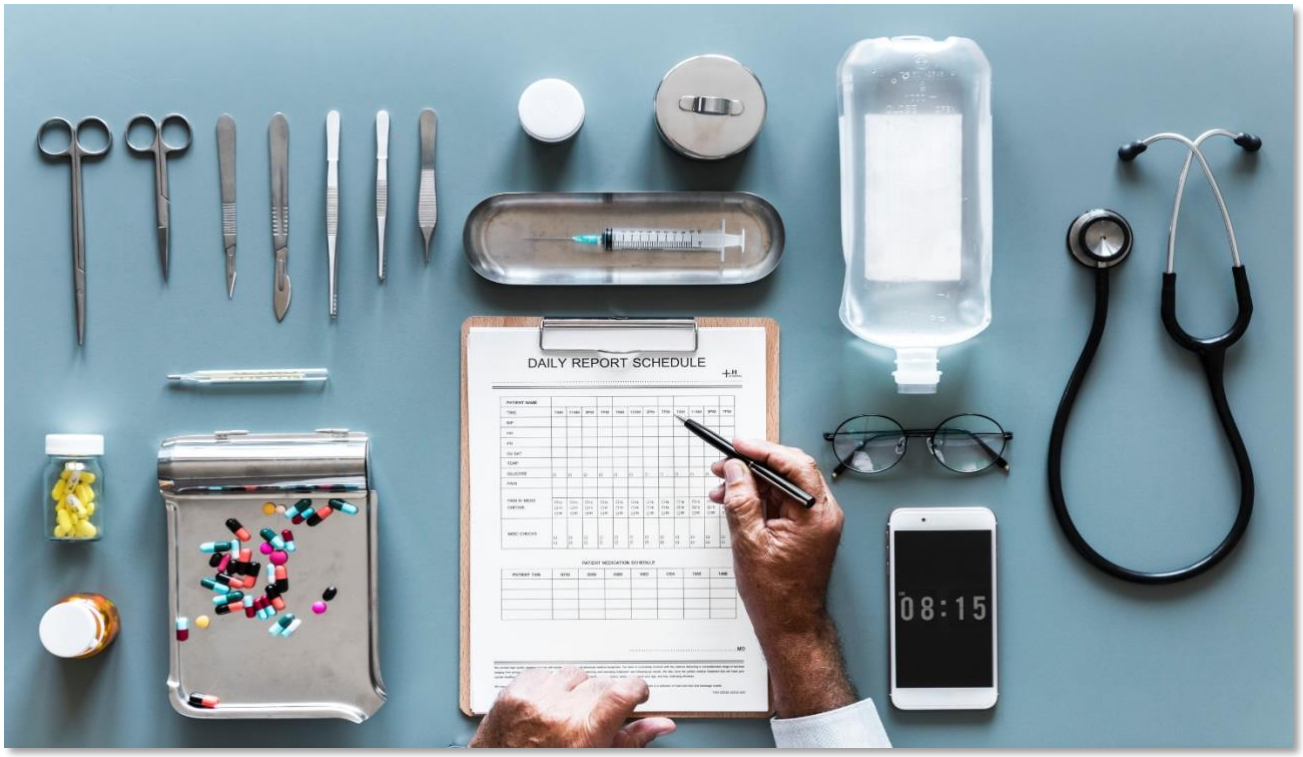
Most data processor agreements therefore clearly state that if the processor identifies a data breach it must contact the controller immediately, and that the processor must never communicate with the Data Protection Authority or data subjects itself. Communicating with the press is also best left to the controller.

In contrast to controllers, which by law are given up to 72 hours to notify the supervisory authority in normal circumstances, processors are expected to inform the controller immediately if they identify an infringement. This enables the controller to start performing its role directly. Contracts often require that the processor responds within 24 hours, although the law actually states 72 hours.

Deciding which communications and which notifications are necessary will not always be straightforward. Failure to give notification of a data breach is an offence and exposes the controller to potentially very large fines. At the same time, the list of notifications of data breaches is public information. No companies want to be included in this list, particularly if it is subsequently discovered that no data breach occurred, or the data were so well protected that there was no risk of damage. Your image may suffer a great deal before this comes to light. Conversely, no company wants to have a reputation for attempting to cover up serious problems. In that respect, openness and transparency are always the best policy.

The authorities might issue further guidelines to clarify when notification is appropriate, and when it is not. Privacy specialists also warn of the danger that, in an effort to avoid fines, companies might report borderline incidents too soon, overwhelming the authorities with notifications that they cannot check and process. A similar situation occurred a while ago in the Netherlands, for example, when the notification obligation was first introduced there in the form of national legislation.

We recommend that anyway all incidents are recorded in the internal incident log, which has to be maintained under the provisions of the GDPR, detailing the established facts, the impact and the remedial action that has been taken. You can also document your line of reasoning for not reporting the incident or not informing the data subjects, for example. This will enable you to demonstrate at a later stage that an incident had been spotted and adequate measures were taken. Following up incidents in this way also goes a long way to improving your procedures and protection measures.



8. The data subject's rights

8.1. The right to be informed

In previous chapters of this book we mainly discussed the obligations which the GDPR imposes on companies and organisations that process personal data. We considered the legislation primarily from the perspective of the controllers and the processors of personal data. It is now time to shift our focus to the individual data subjects.

One of the main aims of the GDPR is to specify your rights as an individual[26] with respect to the vast amount of circulating data that concerns you and is used by others. As a data subject, you can keep a grip on this information, although your rights are not absolute, as we will see.

One of the most important concepts in the GDPR is **transparency**. Every processor of personal data must endeavour to be open with the persons to whom the data relate. It must be easy for data subjects to find out which data are kept and processed by the processor, what the processor does with the data, and why these processing operations are necessary. The processor must be able to explain this in clear and plain language. Within Chapter 5 of this book contain a detailed consideration of how companies and organisations can supply this information in the form of a **privacy statement** on their websites, for example.

The processor needs ensure that you, as a data subject, are properly informed **in advance** of its intentions, the possible consequences and the risks to which you are exposed, particularly if it requests data that it intends to keep and use. It must explain how the benefits of this outweigh the drawbacks for you too.

Moreover, the controller must state **what you can do if you have a question or complaint**. You must be provided with a direct point of contact within the organisation. In addition, the processor has to inform you that you can lodge a complaint about a processing operation with the Data Protection Authority. Obviously, if you lodge a complaint you need to have a valid reason for doing so.

[26] Article 12-15; Article 23 : Recital 58-64

Besides the right to general information, as a data subject you also have specific rights when it comes to your own personal data. Anyone may contact a controller **to access the personal data that the company or organisation keeps on them and to obtain information about the processing operations for which the data are used**. Such 'simple' requests can create a great deal of work for the company or organisation.

Being able to respond accurately to such request's means being thoroughly prepared and following a clear procedure, not least because under the GDPR the data subjects are entitled to receive a response within one month. The controller must either supply the requested information by that deadline or provide a plausible explanation for why it needs more time.

There are several major stumbling blocks that have to be overcome in order to fulfil this obligation. First, the controller must know where the information can be found. This is not a problem when it comes to files with contact details in a CRM application or personnel data stored in an administrative system. Unfortunately, a great deal of information is stored as unstructured data in paper files, in digital files that are not covered by the document management system, or at a local level by individual employees. Gathering such data is much more difficult. Furthermore, the GDPR explicitly states that this service must be free of charge, except in cases where the requests received are manifestly unfounded or excessive.

That being said, this **right of access conflicts with other rights and interests**. When providing information to a data subject, the controller must ensure, for instance, that it does not violate the rights of other data subjects. For example, it will be virtually impossible for a company or organisation to agree immediately to an individual's request for access to all documents and e-mails in which he or she is mentioned. This is because such documents include information about other data subjects, whose privacy must also be protected. Some sources of information also contain other confidential data, which could damage the company's interests if disclosed. In all such situations, it will be necessary to weigh up the different rights and reach a balanced viewpoint. The outcome may be that a data subject's request cannot be complied with. In that case, the data subject must be informed of the reason.

Besides the right to be informed, data subjects have many other rights under the GDPR. These will be discussed in the next chapter of this book.

8.2. Rights concerning own data

In the previous chapter of this book, we discussed the data subject's right to be informed. Every data controller must provide transparent information about the type of data it keeps, the processing operations for which the data are used, and the purpose of those processing operations. In addition, every data subject has the right to access his or her own data.

However, the data subject's rights (and therefore the obligations imposed on the controller) go much further than this. A data subject may also **request that you rectify, supplement or even delete data that you keep on him or her**[27].. The data subject's right to have data deleted is not absolute, and the possibilities for complying with this request must be weighed against other rights and legal obligations. Where there is a legal obligation to archive data for a specific period of time, the data obviously cannot be deleted at the request of a single individual. Sometimes data must be kept for a while in order that all contractual obligations can be fulfilled.

[27] Article 16-23 : Recital 65-73

Moreover, data controllers have to keep a limited amount of data, so they can document their compliance with requests from data subjects for the deletion of data.

Needless to say, the right of rectification is also relative. Obviously, an evaluation report that is kept on file cannot be modified simply because an employee request this. In such situations, employees can exercise their rights by adding comments instead. Rectifications or additions are to be expected - and can even be useful - when data are obtained through third parties, for example. Matters become much more difficult from a legal perspective, however, when it comes to the enrichment of data by the controller that could constitute the controller's added value.

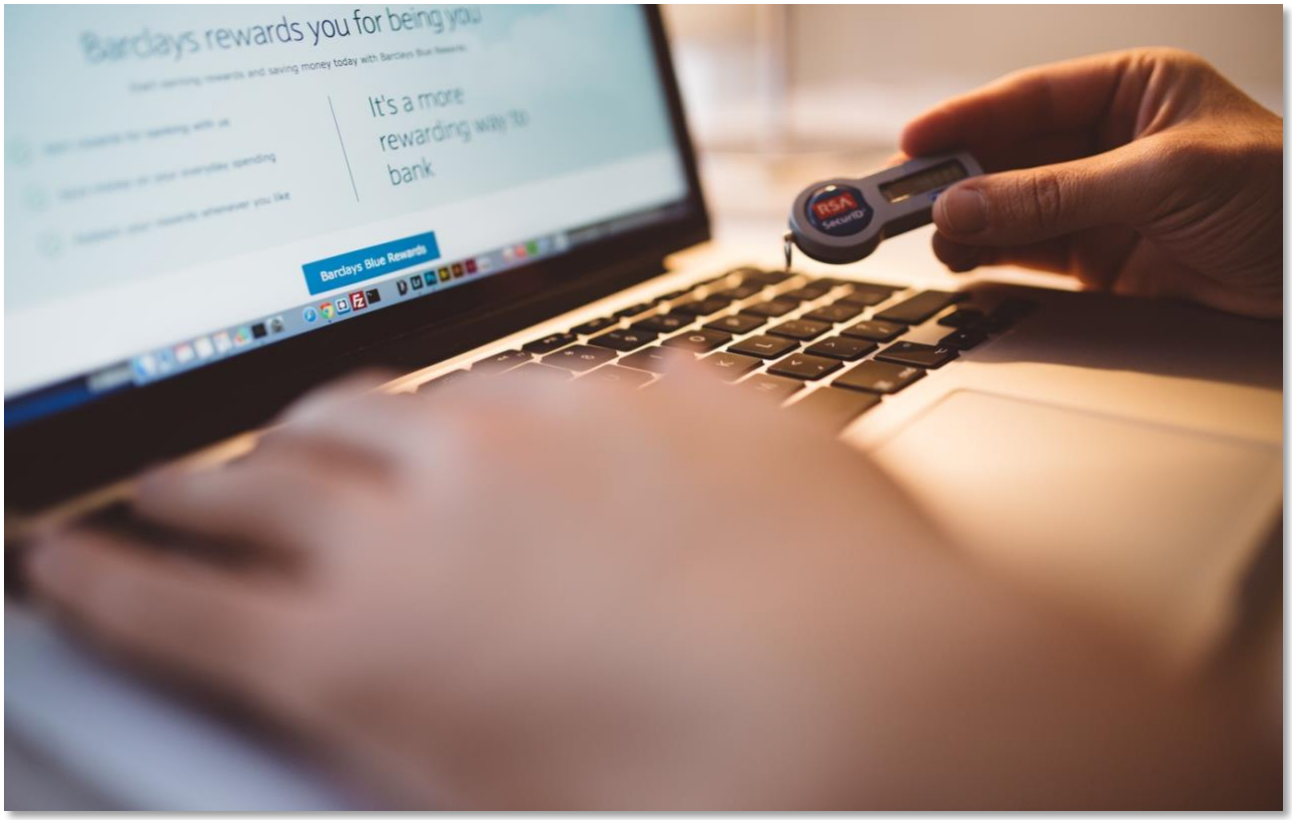
As a rule, any requests to modify or delete data are also applicable to all third parties to which the data were passed on (such as partners or subcontractors). The controller must guarantee that such third parties are also informed of such requests wherever possible. The well-known right to be forgotten has already been the subject of a number of high-profile legal proceedings relating to social media. Clearly, complying comprehensively with requests of this kind is not at all simple. Given this, contracts concluded between controllers and their subcontractors should specify that data is to be deleted immediately following processing.

A data subject may also **request that the further processing of his or her data be stopped or suspended** even though the data are retained. This approach may be appropriate in the event of an ongoing complaint that is awaiting a decision by the relevant authorities, for example because the data subject has contested the lawfulness of the processing operation.

A request of this kind obviously cannot be complied with if the relevant processing operation is performed on the basis of a legal obligation or as part of the duties of government. As we discussed in a previous chapter of this book, processing performed on the basis of consent provided by the data subject can be stopped at any time if the data subject **withdraws this consent**. In that case, the controller must also delete the data.

Finally, the data subject also has **the right to data portability**. This right was already included in the ePrivacy legislation, which imposes obligations on digital service providers. The underlying aim of this right was preventing customers who want to switch service provider from being 'held hostage' by their existing service provider owing to the fact they would lose all their data. After all, no one wants to lose all the photos, books and e-mails they store online. The same right has now also been included in the GDPR and is applicable to all personal data processing operations.

In this much broader context, data portability is often not feasible in practice. Moreover, it leads to conflicts with other rights. For example, a controller that has performed complex operations on data (some of which may be based on algorithms that are the company's intellectual property) will not want to reveal those results without good reason. The interpretation that is most commonly relied upon is therefore that the right to data portability is only really applicable in the case of data that the data subject made available to the processor in the first place.



Tip:

Organisations are advised to establish a proper procedure for dealing with all of these requests.

- First, the contact point for any questions, as well as the responsible person within the organisation, must be made clear to the data subjects. This information can be included in a privacy statement, for example.
- Within the organisation, requests must be passed on quickly to the correct person for further processing, which means everyone needs to be aware of the procedure.
- There needs to be a clearly defined method for establishing whether the identity of the person making the request is the same as that of the data subject whose data is being requested. It is usually recommended that the organisation asks the person making the request to provide a photocopy of his or her identity card.
- There also need to be rules for determining not only which information can be supplied, but also, where applicable, which information cannot be provided, for example because it could include confidential data about other individuals or business secrets. The lines of reasoning that are to be followed must be documented. As part of this, the rights of everyone concerned must be dealt with in a balanced way, since the data subject's rights are not absolute.
- A monitoring system has to ensure that all requests are dealt with promptly and that documentation concerning the progress made and decisions taken is kept.

Clearly, the exercising of these rights will lead to practical problems for data processors. In some circles there are also concerns that the law will be used by data privacy activists to target companies by bombarding them with mass organised requests. However, the GDPR does offer some protection against this by specifying that the requests must not be unfounded or excessive (for example because the requests are made repeatedly). Controllers are not required to comply with any requests that they can prove to be unfounded or excessive.

Despite the above, the fact that we, as individuals, will, at least to some degree, continue to be in control of the information that exists on us, and that companies and organisations will have a framework for handling personal data in a respectful, careful manner, is, of course, a development that is to be welcomed.

9. Accountability under the GDPR

Now that we have essentially covered all of the GDPR, there are a few matters remaining that need to be considered at a more global level. One of these is the accountability[28] of processors and controllers in particular. Everyone who processes personal data must comply with the requirements set out in the GDPR and must also be able to demonstrate and prove that the requirements have been complied with. If you are familiar with audits, you will know what this involves. After you have explained by what means you ensure compliance with specific obligations, you also need to demonstrate that you actually follow the relevant procedures and adequately monitor how they are performed by your employees. This is the subject of this chapter of our book.

A great deal of administrative work is involved in demonstrating that you are familiar with, and understand, all aspects of the GDPR, and that your own organisation complies with the requirements. Implementation needs to be pragmatic yet comprehensive, especially at small companies, organisations and associations. You can find many tips on how to do this in previous chapters of this book. Moving forward, you will need to keep your documentation up to date.

First of all, you need to make sure **sufficient knowledge is available in your organisation**. At organisations with a data protection officer (DPO), responsibility for this is entrusted to the DPO and his or her staff. Even if you do not have a DPO, you still need to be well-informed and provide training to your employees.

The records of personal data processing operations are central to demonstrating compliance. You are required to keep these records under the GDPR, but at the same time they form an ideal starting point for documenting how you ensure data protection. For every processing operation that is described, you need to show that you have thought about the processing operation's purpose and legal basis, and that you have weighed up the risk of a data breach and have taken all appropriate security measures. Of course, you also need to develop a proper procedure to guarantee that this information remains complete. Every additional processing operation must be entered in the records. The DPO has an important role to play here. He or she provides assistance and monitors whether the procedure is performed precisely and promptly.

[28] Article 5.2; Article 24 : Recital 74

For important projects, this preliminary examination can be further formalised in the form of a data protection impact assessment (DPIA).

This is a formal analysis of a processing operation that is aimed at identifying all potential risks of privacy infringements, listing all protective measures and determining whether the processing operation's purpose and legal basis outweigh the remaining risks. If an intensive processing operation involves special categories of personal data, a DPIA has to be submitted to the Data Protection Authority (DPA - in Belgium this is the former Privacy Commission).

Of course, all **measures taken in the area of security** must be properly documented too. When a data protection audit is carried out, you are expected to be able to demonstrate immediately which procedures are applicable, when the most recent version dates back to, the employees to which each procedure is applicable, and whether these employees have been notified and know what to do. If any procedures include recurring checks, it is important to establish one way or another that these checks are actually performed. It is best to keep technical log files and monitoring reports for some time. If manual checks are carried out, you need to produce a short report or keep a log, for instance, so that you can show when these checks were performed and who performed them.

In addition, the entire security system must be evaluated on a regular basis (at least once a year) and adjusted to reflect changes in the organisation, the tools and techniques used or the available security solutions.

In this context, you need to pay special attention to **logging incidents and data breaches in particular**. Every situation that is in conflict with the normal security procedures and every finding that exposes the existence of the risk of a data breach must be recorded accurately in an incident log. Obviously, the items entered in this log need to be investigated in further detail to determine their underlying cause. At the same time, action is planned with the aim of reducing the risk. Examples of action that may be taken include additional technical security measures, additional or modified procedures and checks, and new forms of reporting or logging. This needs to be documented so that you can demonstrate your accountability. While you do not necessarily require a complicated monitoring system for this purpose, at the very least you must have several well-organised logs containing information on all incidents (including their analysis and the agreed remedies) as well as all action items, their status and the individual to whom responsibility has been assigned.

Special attention needs to be paid to the **contractual agreements with partners or suppliers**. You need to conclude data processing agreements with subcontractors to ensure they also comply adequately with the legislation. It is a good idea to keep records of subcontractors that have been entrusted with your personal data processing operations, in which you specify precisely what each subcontractor has been instructed to do and how you have reached agreement about this.

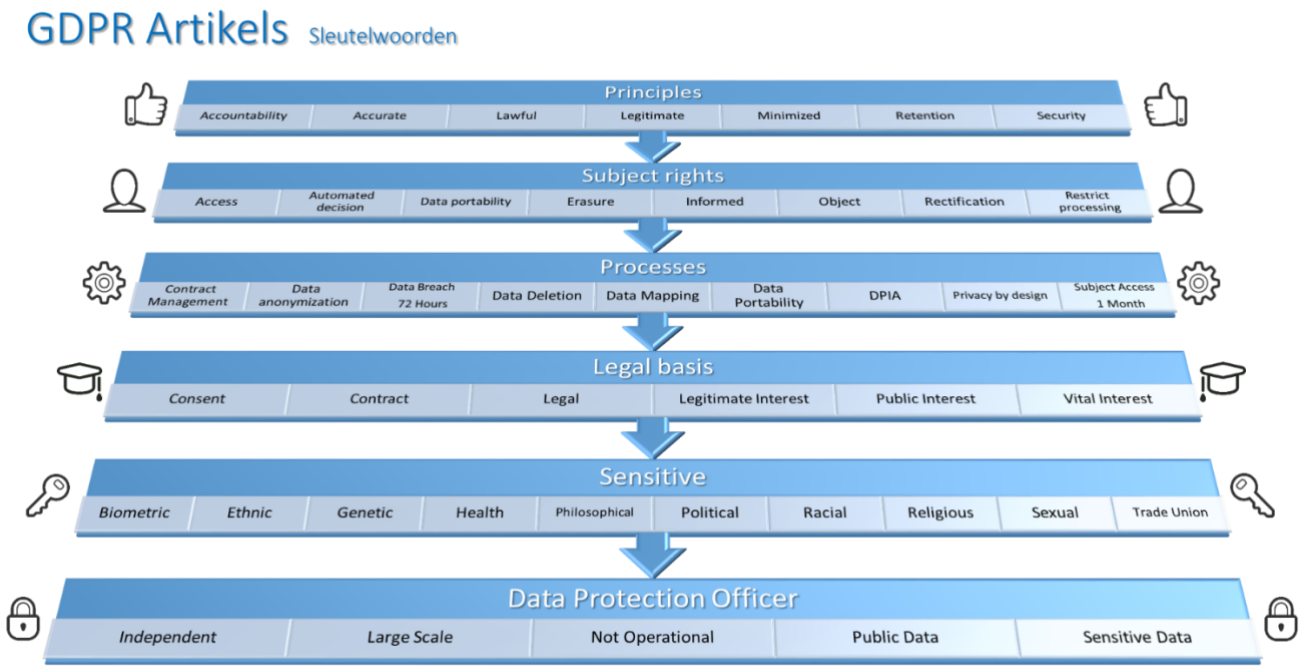
This can then be linked to a specific contract. Conversely, you also need to ensure that your own house is in order **if you are a processor acting for a client**. The processing operations need to be entered in your records, although as the processor you are not required to enter as many details as the controller. In this case, too, it is essential that all crucial agreements are included in a data processing agreement.

Finally, you must be able to demonstrate that you are **able to guarantee the rights of data subjects effectively**. There needs to be proper agreement on the procedure to be followed if a data subject asks questions. It is best to keep records of some kind of all the activities you perform in this context.

If you keep records of every request received from an individual, noting the date and time it was received and all action subsequently taken, you will be able to monitor whether you have reacted in time and responded appropriately. It also means you will always be able to demonstrate that you comply with the legislation to the best of your ability if you are audited by the DPA or in the event of a complaint. Keeping a record of the line of reasoning that was followed is crucial, particularly if you are unwilling or unable to comply with the request.

Simply complying with the legislation is therefore not enough. You also have to document this and be able to prove it. Finally, it is crucial that anticipatory action is taken at the start of all future projects to minimise potential risks. This will be the subject of the next chapter of this book.

For those who are looking for more buzzwords below an overview of all the keywords that are in the 99 articles on the General Data Protection Regulation within their proper context.



10.The future – privacy by design

As we reach the end of our long journey through the world of data protection, we have one final aspect to consider: privacy by design[29]. The legislature wants all processors to take the right to privacy into consideration when they start planning personal data processing operations in future.

The GDPR drafters assume that we will develop some kind of privacy reflex. If we do, the legal requirements will become a natural, self-evident aspect of building an application or configuring a website, or, equally, organising a survey or setting up a scientific study.

It is best not to collect or process personal data except where necessary. And even when we do have a good reason to collect and process such data, we need to **limit processing operations to those that are strictly required**. All new initiatives therefore require plenty of thought.

- While it may have been considered advisable in the past to add more attributes or fields to a file when performing an analysis for a new application or designing a database, on the basis that they might come in handy in future, today it is more important that the amount of data is minimised and geared to the specific purpose for which the data will be processed.
- It is advisable to include information in a database to indicate when a specific piece of data is out-of-date or obsolete, or simply may not be kept any longer. This makes it easy to delete data systematically when no longer needed or if we are no longer able to guarantee the data's accuracy.

[29] Article 25 : Recital 78

In future, applications might contain a functionality to guarantee **the data subject's rights** and make it easier for these rights to be exercised in practice.

- Whenever an application requests personal data from data subjects, information about the purpose for which this is done, the duration of the processing operation, the risks entailed, and the protection measures must be made available at the same time. A smartphone app that records athletic performance, for example, must provide the data subject with adequate information about the data it collects and stores in the background, and what the builder of the app intends to do with the data, before he or she uses the app for the first time. It should be possible to incorporate this in a convenient manner in app user interfaces.
- In the same way, everyone attempting to gather data through a website must immediately provide clear background information on the processing operations. Such information must be provided in a timely manner. Distinctions must be drawn between different potential purposes insofar as possible.
- Future applications could also include a functionality that allows data subjects to view their data, and, if the situation permits, rectify, supplement or delete the data. Of course, this is only possible if the data subject's rights do not conflict with other interests.

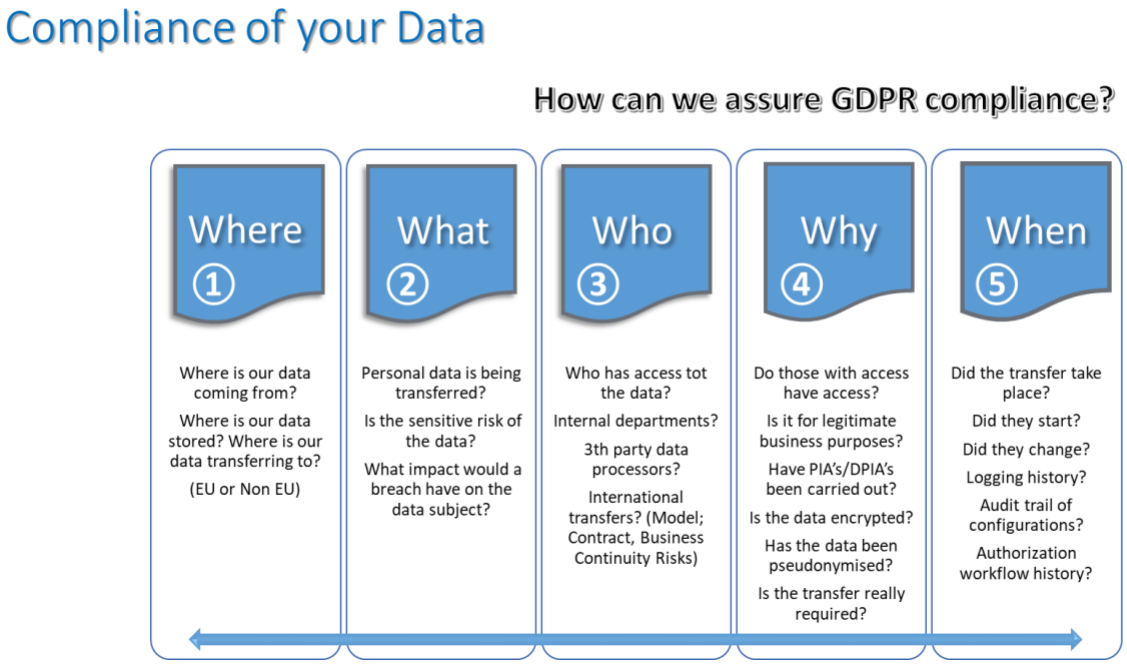
Privacy by design also means that when an application is designed, **the best ways to protect the data** are considered from the outset.

For example, you can build the application in such a way that everything is encrypted where possible. A website can use encryption protocols such as https, and data can be exchanged by means of encrypted files sent through encrypted channels. If any data have to be kept for some time following a processing operation, they can also be kept in an encrypted file, for example in a secure digital archive. All of these measures reduce the risk that data will be made public or fall into the wrong hands. Taking such measures into consideration from the start of the design phase will work out much cheaper than having to make changes later on.

Another measure that may also be considered in some circumstances is data pseudonymisation. As we explained in an earlier chapter of this book, this means removing the direct references to specific individuals from the files. It also reduces the risk of infringements in the event of a mishap involving a file.

This brings us to **privacy by default**. What this means is that whenever an application allows the user to choose whether or not to make data public, share data with others or make data available for certain types of processing operations or future communication, the standard settings of that application must always be its most secure settings. These settings are changed only if the user actively performs a procedure (such as ticking a box or clicking on a button to indicate consent).

As you can see, maximum data privacy can be ensured using all kinds of measures, which the GDPR encourages everyone to apply at all times and to the greatest extent possible. Data privacy is therefore not a stand-alone subject for a topical project that we can soon forget; on the contrary, it is a matter of constant concern. One thing is clear, however: data privacy is something that needs to be taken into consideration and this will most probably always be the case.



11.GDPR – The immediate effects

On 25 May 2018, the General Data Protection Regulation (GDPR) came into effect. This new European legislation sets out how businesses, authorities and organisations are to handle personal data. The time has now come for us take a pragmatic look at the tsunami we have had to ride during the past few months.

One of the first observations is that it took a long time for things to get going. This is striking given that the GDPR did not come as a surprise. The fact that this legislation would be introduced had been known for years, and the official text was published as far back as April 2016. It therefore is astonishing that so many businesses knew little, if anything, about the GDPR and that they only started to get organised at the beginning of 2018. Does this go to show that most organisations do not take privacy and data protection seriously? Or was it down to genuine ignorance?

Most of the activity we have seen has been in two areas. First, many controllers, which are responsible for the processing of personal data, took the GDPR as an opportunity to contact the individual recipients in their address files or other individuals on whom they gather information. And second, data controllers and the businesses that process personal data on their behalf are holding intense negotiations. We will consider both phenomena in further detail below.

11.1. Communication between controllers and data subjects

Virtually all of you will have received a deluge of emails and letters about data protection from businesses and organisations in the run-up to 25 May and afterwards. Some asked for consent to use your data, some of them simply mentioned that their privacy statement had been changed, and some of them explained which information they keep about you and why they are justified in holding that information. In any event, the date did not pass unnoticed.

The unintended consequence is we now have mailboxes full of messages that we did not ask for and are often uninterested in. They are annoying, but do they improve data protection?

At the very least, it is worth identifying who has information on us, as there are bound to be some surprises. In many cases, it is not clear how a controller got hold of our contact details. If we go to the effort of reading all those communications, we will in any event be aware of the processing operations carried on by those firms or organisations. Transparency has increased – and this was one of the objectives of the GDPR.

It is very interesting to see how many different approaches exist, as there have been many campaigns designed to **ask data subjects for consent**.

- Sometimes this is done in a completely pointless manner. Businesses write to data subjects in order to obtain their consent for the processing of their data. They provide some clarification, and they end the communication by stating that consent is deemed to have been given unless the data subject contacts them to unsubscribe. It goes without saying that this is illegal under the GDPR. Tacit consent is no longer sufficient. An affirmative act must be performed, and the controller must also be able to demonstrate that data subjects were aware that they were giving consent. This means that there is no legal basis if the data subject does not respond to the request for consent.

- As a data subject, you occasionally come across an excellent example of how things can be done. You are presented with a link to a site containing plenty of information, where you can find every element of a proper privacy statement: the purpose and legal basis of the processing operations, the length of time for which the data are kept, possible recipients, the security measures and so on. Sometimes you also get to see the information the firm keeps on you and you can even correct or supplement this information data yourself. There is also a clear explanation of your rights and how you can exercise them. It goes without saying that you are also able to request the deletion of your data. These are outstanding examples that demonstrate how things should be done.
- A major question concerns what should happen if a data subject fails to respond to a request for consent. From a legal perspective, this must result in the deletion of the information and the ending of all communication, since the legal basis selected by the controller does not exist. But will firms make repeated attempts to obtain consent? And if so, how many attempts can they reasonably make? Only time will tell. Moreover, is it really the case that we will not receive any further communications?
- Will we see turbocharged slim-down campaigns, in which megabytes of messages simply vanish into thin air? Unfortunately, we do not think this is likely. Ingrained commercial activities will carry on as usual, with or without the GDPR. And as you will no doubt already have concluded, the GDPR is not an anti-spam filter.

Other controllers opt for the alternative route when contacting data subjects. They rely on having a **legitimate interest**. In such cases, they do not require the data subject's consent, and their communications ensure they provide the transparency required by law.

As long as their campaign provides sufficient information on the specific processing operation and its purpose, and data subjects are clearly told how to exercise their rights, and in particular how to indicate that they do not want their data to be processed, this is sufficient for the purposes of the GDPR.

The use of personal data for **e-mail communication** is a key concern. This is covered by the GDPR and another EU directive, the **ePrivacy legislation** (2002/58/EC and 2009/136/EC). The EU intended to convert this legislation into a new regulation and harmonise it with the GDPR, but the completion of this revision process is still a long way off, partly because many discussions and heavy lobbying are still taking place. It is therefore unclear which direction we will ultimately move in.

The current e-Privacy Directive is stricter than the GDPR and explicitly requires that the data subject's consent is obtained for e-mail communication for direct marketing purposes, unless the data subject is a customer and the services or products that are offered are similar to goods or services previously supplied to the data subject. More recently, the professional associations of marketers in the Netherlands pointed out that their businesses would be in peril if this legislation were to become too strict.

Of course, the data subject's rights continue to apply in this situation, too. You can ask a firm to stop processing your data at any time, even if the controller believes that it has a legitimate interest in doing this. If there is no legal obligation to process your data, or a storage period is not prescribed by law, the data must be deleted or, at the very least, must no longer be processed. This means that even if an organisation has opted to use a legitimate interest as its legal basis, it still needs to develop the necessary measures so that it can comply appropriately with requests from data subjects to stop processing their data. This is quite a task.

11.2. Contracts and agreements between businesses

Another area where developments have been seen concerns the contractual agreements reached between controllers and the companies they engage as subcontractors for processing operations. This is because under the GDPR the controller remains liable and must guarantee that any supplier it engages also complies fully with its legal obligations. This must be recorded in a way that can be verified.

We know from personal experience that concluding processor contracts with all clients and suppliers (where necessary) is a huge task. Although many organisations have already made a start on this, there are still plenty of contracts that still need to be signed.

The Belgian federal government has also attempted, through its departments, to gather together all the different kinds of data processor agreements and incorporate them into a general template for all towns and municipalities in the Flemish Region. However, a one-size-fits-all solution has not yet been found. It is also extremely difficult to apply a genuine single standard. Clients cannot be forced to accept this, particularly if those clients are large organisations. Major suppliers also put forward their own texts. The inevitable upshot is that dozens of legal texts have to be read and screened for completeness and balance.

A number of issues crop up time and time again.

- Is it possible to limit liability or not? The fines alone can be massive and estimates of the direct, and in particular indirect, damage in the event of a serious data breach are often very high. While it seems reasonable that clients should want to avoid putting their suppliers out of business, stipulating that liability is to be limited to the sum insured under a cybersecurity insurance policy is not so easy in many cases.
- How far should the right to perform audits extend, and what about costs of hosting an audit?
- Is it realistic to pass on the task of responding to requests from data subjects to subcontractors, and if so, to what extent is this the case? For example, is that feasible in the case of a processor that sends batch communications?
- Is it reasonable for a client to require that additional work arising due to obligations under the GDPR is performed by the supplier free of charge because this work needs to be performed in order to comply with the law?
- How should you deal with the fact that a controller has to give a processor specific approval to engage a sub-processor? Does this mean you, as a processor, are no longer able to direct your own business operations?

For some of these issues, it will be necessary to come to more balance arrangements that are more economically viable. At any rate, careless handling of personal data could be punished severely. As a processor, your best course of action is to comply with the main elements of the new legislation. Looking ahead, information security and data protection will become an inevitable fact of life for all companies providing services that involve the processing of personal data processing, just as quality already has.

12.GDPR – Expected consequences

The last chapter looked at the immediately perceivable impact of the GDPR's introduction. In the past two years, however, several other significant consequences have also been suggested, mostly by lawyers and consultants seeking to create business by pointing out major threats. These consequences include massive fines, a duty to report incidents and data breaches (which could lead to the reporting party being put in the pillory), and a deluge of requests from individuals wanting to exercise their rights relating to their data. We can only conclude that so far things have not been so bad, but that might be because the mechanisms have got off to a slow start. In any event, the positive effects of the legislation have been the most notable to date.

12.1. Fines

What about the fines imposed in the event of failure to comply with the GDPR? These amount to up to € 20 million or 4% of your business's total worldwide turnover, but what exactly does that mean, and which of these amounts is higher?

To put this in perspective, 4% of income (for 2016) amounts to $5.44 billion for Amazon, $3.6 billion for Google, $1.1 billion for Facebook and just $352 million for Netflix. You can calculate what 4% of your own business's income is for yourself.

You will often hear GDPR non-believers making comparisons with the infamous millennium bug (also known as the Y2K bug) at the turn of the 21st century. It was claimed that the world would come to an end because computers would stop working on 1 January 2000, catapulting us back to the Stone Age. Fortunately, things did not turn out that badly, and the impact of the millennium bug was relatively limited. Comparing this situation with the GDPR, however, would be an oversimplification.

Nevertheless, 25 May 2018 has been and gone, and, as far as we are aware, no fines have been imposed so far. The Belgian Data Protection Authority, which is tasked with setting and imposing fines, has not yet completed the implementation activities for the application of the new regulation. That said, we certainly do not want to create the impression that you can safely rest on your laurels.

12.2. Duty to report data breaches

With effect from 25 May 2018, all data breaches involving personal data that occur within the EU must be reported in accordance with the GDPR. The duty to report data breaches means that organisations (such as businesses and public authorities) must notify the Data Protection Authority (e.g. the Dutch Autoriteit Persoonsgegevens or the Belgian Data Protection Authority) as soon as a serious data breach occurs – and no later than 72 hours after they become aware of the data breach. As a business, you therefore only have three days in which to report incidents to the authorities and find out the circumstances of a supposed breach of privacy.

When reporting a data breach, you must to explain: 1) how the data breach came about; 2) which measures you will take to ensure the data breach cannot happen again; 3) how and when you will notify the affected parties. If there is a serious risk of damage, you must also inform the data subjects (this means the persons to whom the leaked personal data relate) about the data breach.

In the Netherlands, this duty to report data breaches has been in place since 2016, and it is interesting to see how many potential data breaches within organisations have been reported. In 2017, approximately **10,000** breaches were reported, and in **47%** of those breaches personal data was sent or given to the wrong recipient. The most frequently leaked pieces of information were the data subject's name, address, gender, date of birth and/or age, and citizen service number.

Surprisingly, **298** reports were withdrawn because it was subsequently discovered that a data breach had not actually occurred. If you would like to know more, the full report can be downloaded as a PDF file from the website of the Dutch Data Protection Authority.

The obligation to report data breaches is now in effect in all EU Member States. If you would like to find out more about how the process works, visit the website of the Belgian Data Protection Authority and try to log a report of a fictitious data breach. Good luck with that! In the Netherlands, the Dutch Data Protection Authority has a better grip on things, but it has had an additional 18 months to become used to this new duty to report data breaches.

12.3. Exercising of data subject's rights

We now know what the data subject's rights are. As a private individual living in the EU, you can ask any organisation for a comprehensive list of all the information it holds on you. Moreover, you can ask the organisation to transmit this information in a format that is transparent and is easily readable. You also have the right to be forgotten, apart from by the tax authorities or in situations where general legislation in your country land stipulates otherwise (for example in the case of accounting information that must be kept for at least seven years). The collector and/or processor of the data must respond to such requests within 30 days.

However, I sometimes wonder who among us will actually exercise this right in practice, apart from those of us who like to put businesses or associations to work by forcing them to find out exactly where our information is kept. Perhaps you have valid reasons for doing this, and there will certainly be circumstances in which it is warranted. It will, however, probably be the exceptions that prove the rule.

The GDPR was, admittedly, introduced too recently for any conclusions to be drawn at this time, but will we really all assert our rights when it comes to ensuring our information is stored correctly and securely by third parties in the cloud? And who will check everything on our behalf? It is unlikely to be the Belgian Data Protection Authority or Dutch Data Protection Authority, because both of them have their hands full already.

On the other hand, many companies at this point are certainly not yet well prepared. A recent survey by Talend SA, of which Datanews and Techzine reported, tested from June to early September 2018 how companies would respond to requests from stakeholders to transfer their data. Less than half met the regulatory requirements. Only a few technologically advanced firms had a nice and fast solution. So, there is still work to be done.

12.4. Positive developments

We must not forget the positive developments that the GDPR has led to. The new legislation is an opportunity to put your business in order as regards the handling of information. You can do this by taking a critical look at the amount of data held by your organisation and by applying a data classification system.

Ask yourself at the outset who can access the information and where the information is located. These are the first steps you need to take in order to change your information policy. Questioning why you keep specific personal data and what you, as a business, do with that information can help reduce the risk you would run in the event of a data breach. After all, prevention is always better than cure. By doing this, we gradually learn questioning the need to process data before we start collecting them.

In addition, we also notice that almost all of the companies have made their privacy statement. Thanks to the GDPR and all the attention that data privacy is given, it creates a greater transparency around the collection and processing of personal data. Information about it must no longer be sought for in the small print of contracts. Companies make it a point to their clients, and other contacts to report what data they maintain about them and why this is necessary.

Within many organizations, the GDPR was an opportunity to make their staff more aware of risks that can lead to a breach of the security of information. Not only sophisticated hacking programs threaten the data for which a company is responsible, but also inattention or carelessness of the employees.

The more important data become, the more weight will be given by data controllers to trust as a differentiator between potential data processors they want to engage.

More insight into the importance of data privacy and the potential consequences of errors contribute certainly to a higher level of safety. Once you are compliant within your company in terms of information security, you can make this known on the basis of a kind of quality label. So, you can mention the professional approach in dealing with person-identifiable information of your customers but also to your own employees.

13.GDPR – An obstacle to technological progress?

Besides all the other effects that the GDPR has, the imposition of this new regulation could also have unintended consequences when it comes to one of the most profitable sectors in our global economy: the technology sector.

13.1. Additional costs and additional conditions imposed on start-ups

First, costs will increase, causing a fall in profitability, which in turn will lead to lower profits and ultimately lower levels of investment, fewer start-ups and slower growth in this sector.

Another potential consequence is that the GDPR could limit access to technology for private individuals and businesses in Europe. Many of today's apps are made by small businesses that collect a great deal of personal data. All internet start-ups dream of seeing their number of users reach the one million mark, and they try to achieve this goal by going viral with software that is inexpensive, and in many cases available free of charge. Their business model is to collect information with the aim of using big data to create value.

Today, however, they also have to comply with the GDPR because they keep and process personal data related to persons living in the EU. As such personal data includes IP addresses, geolocations, home addresses and e-mail addresses, all of which are bound to be collected, internet start-ups will have to ask every user to give their consent.

13.2. Digital borders

Since 2017, the rate of cloud adoption in Belgium has grown steadily (see also our Cloud Barometer), and today one in five apps runs directly in the cloud. This year, 2018, almost every self-respecting SME will study cloud solutions in much greater depth, or will obtain guidance from its preferred IT supplier in order to make the most of the benefits offered by cloud solutions. We are often asked to provide advice in this area as not everyone has developed a good understanding of the cloud yet.

One of the most frequently asked questions is invariably: "Is the cloud safe, and how can I, as a manager, check this?" In particular, the difference between public and private cloud solutions is unclear to many people, and most SMEs have been in the public cloud for a long time without realising it.

Many employees have their own private e-mail or Dropbox account and also have at least one app that they use for social media purposes, such as Facebook, WhatsApp or LinkedIn. More than anything else, this goes to show that the use of such services in the Cloud is well-established.

Almost all of these services are provided by public cloud providers based in the United States. With regard to this phenomenon, I heard the following saying during a visit to a manufacturer:

"America invents it (i.e. Amazon, Facebook, Google), China copies it (i.e. Alibaba, TenCent) and Europe regulates it (i.e. the GDPR)".

This is particularly apt when you consider that all of the major public cloud providers come from the United States (Big 5) and have offered their services for decades, and Europe is now putting a stop to this through the GDPR.

As a business, however, you need to be able to demonstrate that you fulfil the obligations discussed in the previous chapters. When it comes to cloud services in particular, the GDPR is a real challenge because the data relating to your business and users will be kept constantly 'out of reach'.

The new framework imposes obligations not only on the controller, but also on parties further down the chain that process personal data for purposes such as data analytics, storage or billing, the last of which is a significant new development for IT service providers, and, more specifically, providers of cloud services. The GDPR assumes that contracts will need to be amended and data protection policies will need to be drawn up, in accordance with the requirements laid down in the regulation. This is because all businesses need to be able to demonstrate that they handle the personal data of their employees, customers or suppliers in a responsible manner.

Consequently, there are challenges to be faced on multiple levels. If we are honest, many businesses have never stopped to think about data protection. Technology can do a great deal, but applications and processes will need to be re-examined in the light of these changes in the law.

This can be avoided by simply no longer collecting information relating to people who live in the EU. This can be done by asking users to confirm that they do not live in the EU by clicking on a button before an app is installed.

Alternatively, geo-location can be used to block the app completely.

This could however, mean that all Europeans are cut off from the latest software developments. It might be the case that if you want to install the latest secure communication app, this will no longer be possible, or the new business app for managing contacts or keeping your accounts that you like is unavailable in the EU and can only be used by people outside Europe.

This might become a major problem for Europe. Please do not misunderstand me: I am very much in favour of the responsible handling of personally identifiable information and secure data storage in general. However, if the data protection authorities in Belgium or the Netherlands follow the letter of the GDPR when applying the rules, this could throw up new digital borders that the internet and we, as consumers, are not calling for.

14.'Preliminary' Conclusion

Only time will tell how large and small businesses, individual data subjects (possibly goaded into action by consumer organisations or trade unions), the supervisory authorities and the EU itself will deal with the GDPR. There will no doubt be some complex disputes for the courts to deal with. It is therefore hard to predict what the answers will be to the many questions that currently still remain. That is why we cautiously refer to a 'preliminary' conclusion. One thing is clear, however: data protection is something that needs to be taken into consideration and this will most probably always be the case.

One objective has been achieved at any rate. During the past year, the issue of privacy and data protection has been on the agenda of every association, public authority and business. Everyone has thought about the use of personal data. In many cases, this has led to decisions to reduce or phase out databases and substantially shorten the storage period for data. Personal data are now handled with greater care. An atmosphere of openness has emerged regarding this matter. In many cases, the desired level of transparency has been achieved. We will not know whether the results are permanent until the media hype has died down and managers have shifted their focus elsewhere. That said, our impression is that the fact data subjects have the right to know what happens to their data is an achievement in itself. This information is no longer hidden away in small type in long-winded contracts; instead, it is provided in a clear and transparent manner on websites, in emails and in apps.

More consultation is still needed if we are to gradually remove all uncertainties and arrive at uniform rules and agreements, balanced codes of conduct, measurable controls, and contractual texts that can be used by all. However, if we continue with the work that is already under way at many organisations, we can be confident that the current level of uncertainty will decline. Perhaps data protection will become a given throughout the entire European Economic Area, as quality management, environmental protection and sustainable business practices already have.

The most difficult question to answer is whether the GDPR will succeed in its main aim of achieving a balance between the protection of privacy and the right to freedom of expression and the free movement of goods and services. If the regulation has the effect of restricting or impeding new technology relating to the knowledge economy, then things will have gone too far in one direction. However, a balance will not exist either unless the longed-for protection of the data subject is achieved in practice.

It will therefore be necessary for reasonableness to be shown on both sides, between data subjects and companies or organisations, between European institutions and the major market players, between inventive start-ups and their investors and customers/users, and, no less importantly, between Europe and the other global players – because we live in a global economy.

There is therefore every reason to continue to keep a close eye on developments.

We will try to keep you informed about future evolutions through our blogs and maybe by adding new updates to the book.

About the author

Following a brief academic career, Viktor D'Huys[30] started working in the IT sector over 30 years ago. He became the CIO of Group Joos in 2003, and today he is helping to facilitate the digital transformation of the group, which has evolved from a printer into a hybrid communication specialist offering many digital services.

Viktor's specialist areas include IT security. He was responsible for setting up the information security management system (ISMS) that enabled Group Joos to obtain ISO 27001 certification in 2013 and continues to develop the information security policy. It was a logical extension to add data protection to his responsibilities in 2016. Together with the Data Protection Officer, he was jointly responsible for managing the project that ensured Group Joos was ready for the GDPR on time. His blog about data privacy on the Group Joos website was the starting point for this book.

Viktor is a Certified Information Security Officer (CISM) and Certified Information Privacy Professional (CIPP/E).

About the co-author

During the past ten years, Peter Witsenburg[31] has had the opportunity to work in the fields of cloud computing and IT security. In the latter sector, Peter was responsible for carrying out various internal and external ISMS and GDPR audits (based on regulations regarding privacy and data protection).

He has been involved in the implementation of the ISO27001 standard for an ISMS (information security management system) for risk assessments, the information security policy and the business continuity plan (BCP), using the PDCA methodology, at organisations including Interxion.

Alongside his work, Peter serves as the vice-chair of the Selection Committee of vzw *'Netwerk Ondernemen Vlaanderen'.* In his free time, he writes articles and books on the latest trends in IT. Peter is also the founder of 'Belgium Cloud' and 'CloudMakelaar'.

[30] Chapters 1 to 10 were written by Viktor D'Huys and reviewed by Peter Witsenburg, who also supplied the images that illustrate this book.

[31] Chapters 11 to 14 are a thorough reworking of texts written jointly by Peter Witsenburg and Viktor D'Huys. Peter Witsenburg was responsible for the composition and layout of this book.

References

The **official legal text** of the GDPR in English, French and Dutch can be found as PDF via the following links:

http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

http://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32016R0679

http://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:32016R0679

More **background information** can be found everywhere. I shall confine myself here to a few official channels.

The **European Commission** provides more info via the following link:

https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_nl

The website of the **Belgian data protection authority** has been adapted on May 25, 2018. With the old URL (https://www.privacycommission.be) you still will see a transitional page, where you find the new site in Dutch, French or English. The content and structure of the site is about remained the same, but updated with regard to the Organization of the data protection authority.

https://www.gegevensbeschermingsautoriteit.be/)

This site contains a lot of information about the GDPR. You can find a roadmap and a whole series of theme files and the ability to download documents.

https://www.gegevensbeschermingsautoriteit.be/algemene-verordening-gegevensbescherming-avg

The authority personal data (AP), the Dutch data protection authority and the independent governing body that has been appointed by law in the Netherlands as a supervisor to monitor the processing of personal data.

Here you can visit the site of the Authority Personal data (AP) and you can find a wide range of useful information neatly arranged by topic.

GDPR - References articles and recitals by chapter*

1.1		Article 4.1 en 4.6 - Recital 15, 26-27 en 30-31
1.2.		Article 4.13-15; Article 9-10 - Recital 34-35 en 51-56
1.2	Pseudonymisation	Article 4.5; Article 25 - Recital 78
1.3	Data processing	Article 2.1-2; Article 4.2
1.3	Homely atmosphere	Article 2.2c - Recital 18
1.3	Responsible	Article 4.7
1.3	Processor	Article 4.8
1.3	Data subject	Article 12
1.4		Article 37-39 - Recital 97
2		Article 5 - Recital 39
3.1		Article 30 - Recital 82
3.1	Who registry duty	Article 30.5 - Recital 13
3.2		Article 30.1 - Recital 39
4.1		Article 6 - Recital 40-50
4.1	special categories	Article 9 - Recital 51-56
4.2		Article 4.11; Article 7-8 - Recital 32-33,38,42-43
4.3		Article 6-9 - Recital 47-49
5.1		Article 13-14 - Recital 60-62
5.2		Article 12.1 - Recital 58
6.1		Article 24.2 en 25; Article 32
6.2		Article 32; Article 35-36 - Recital 75-76, 84, 89-95
6.3		Article 32 - Recital 77-78
6.4		Article 28-29 - Recital 79 en 81
7.1		Article 4.12; Article 33-34 - Recital 75 en 87-88
7.2		Article 33 en 34 - Recital 85-88
8.1		Article 12-15; Article 23 - Recital 58-64
8.2		Article 16-23 - Recital 65-73
9		Article 5.2; Article 24 - Recital 74
10		Article 25 - Recital 78

**References to the GDPR Articles thanks to intersoft consulting, see also: gdpr-info.eu*

All articles into more details can be found in the following publication:

Regulation (EU) 2016/679 of the European parliament and of the council of 27 April 2016.

Epilogue: Group Joos and the GDPR

Processing of personal data is the core business of Group Joos. That's why we already started the preparation of the GDPR in April 2016, even before the GDPR was published officially. Already at that moment we appointed a Data Protection Officer. It was our duty towards our customers to start collecting information immediately and to make our organisation ready to comply.

For Group Joos it is an absolute priority to adequately protect confidential data. All personal data naturally belong to this category. During the last years Group Joos heavily invested in technology and built in all kind of organisation controls to heighten the level of information security. Already for 5 years we are ISO 27001 certified.

That's why we are confident that Group Joos is ready to be their customers' trusted partner in processing personal data.

If you want to be sure the personal data you are in control of are handled with care, Group Joos is the right partner for you. We can organise your marketing mailing, prepare a multichannel campaign to reach your prospects or even handle very sensitive medical or financial information and deliver documents with such information to the data subjects through the channel of their choice. We have a platform in place to safely deliver the data at our sites, to process the information accurately to deliver it physically or digitally wherever you wish. Optionally we also can store the encrypted data after processing for an agreed retention time. Even a trusted digital archive is a possibility. Group Joos has adequate technological solutions for your communication and can help you with your digital transformation in several ways. At the same time, we are ready to be compliant to all aspects of the new privacy law, in respect to the rights of the data subjects.

Group Joos is keen to share the know-how and expertise in this area with you. We hope the information presented in this publication can be of interest for anyone having questions about the adequate way to handle personal data.

GROUP JOOS Unlimited Digital Solutions & Print

Group Joos nv

Everdongenlaan 14 -2300 Turnhout (B)

gdpr@groupjoos.com www.groupjoos.com

PRACTICAL

GDPR

GUIDE

Responsible Publisher: Group Joos in cooperation with Cloud Makelaar