EXIN Privacy & Data Protection Foundation

Edition 202009

About the authors

Leo Besemer
CertiQA
https://www.certiqa.nl/website/
Contact: leo.besemer@certiqa.nl

Version administration

Version	Changes
201707	Original version
201912	• Changes to reflect that the moment the GDPR fully applies as law and the installation of the EDPB, are now in the past. • Paragraph on the situation between publication and application of the Regulation was deleted. • Update and correction of the list of adequacy decisions (§ 7.5.2). • Status of the proposed Regulation on Privacy and Electronic Communications. • Small textual corrections. • The term 'data breach' was replaced by 'personal data breach' as that is the term used in GDPR.
202009	Added reference to the latest GDPR information regarding the US Privacy Shield adequacy decision.

Content

EXIN Privacy & Data Protection Foundation

Introduction

This white paper presents exam literature for candidates studying for the EXIN exam Privacy & Data Protection Foundation (PDPF). For the most recent exam requirements refer to the official EXIN Preparation Guide, which can be downloaded from www.exin.com.

In a digital era, information about people is becoming more and more valuable. Enabled by new technologies, organizations collect and store data on a large scale. This recent explosion of data presents specific security challenges, especially where personal data are concerned, also due to the stringent regulation of the European Union regarding the protection of personal data.

Privacy, and thus the protection of personal data, must be a priority for any organization.

Organizations processing personal data of people residing in or visiting one of the European Economic Area (EEA) member states must comply with the General Data Protection Regulation (GDPR). Organizations outside of the EEA must also comply with the GDPR when doing business in Europe. Adherence to the GDPR both prevents fines and enhances customer trust.

Having certified professionals with the right level of knowledge can help prepare an organization to comply with the GDPR and help them to stay compliant. The EXIN Privacy & Data Protection program covers the required knowledge of data protection and the GDPR regulation for compliance.

EXIN, October 2019

Privacy fundamentals

1 Definitions and Historical Context

In this chapter we will look at the history of privacy and data protection and the relationship between the two concepts. With that, we will look at some basic definitions as they are used in the General Data Protection Regulation (GDPR). Some of the terms and concepts are explicitly defined in Article 4 of the GDPR. Some of the terms used throughout the GDPR are derived from international law.

1.1 The History of Data Protection Regulations

> Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual … the right 'to be let alone' … Numerous mechanical devices threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the house-tops'.
>
> Source: https://www.brandeis.edu/now/2013/july/privacy.html (as viewed on 18 March 2017)

While one might think that this text has been written recently, Louis D. Brandeis wrote it in an article in Harvard Law Review in 1890. This, in more modern English, right not to be bothered or interfered with, ultimately became the basis upon which Article 12 of the Universal Declaration of Human Rights (UHDR) was founded in 1948.

> No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks.
>
> Source: https://www.un.org/en/universal-declaration-human-rights/ (as viewed on 18 March 2017)

The rapid progress in data processing and the increased possibilities in the use of telecommunications in the 1970s coincided with the development of the European Union, which increased cross-border trade. As a result, a need was felt for new standards that would allow individuals to exercise control over their personal information. At the same time, international trade needed free international flow of information. The challenge is to find a balance between concerns for the protection of personal freedoms and the possibility to support free trade throughout Europe.

The member states of the European Union have, in the European Convention of Human Rights (ECHR, 1950), signed a treaty to uphold human rights throughout the European Union, amongst them the **right to respect for private and family life**.

A first effort to consolidate the **protection of privacy** and the need for **free international flow of personal data** came from the Organization for Economic Co-operation and Development (OECD) in 1980: *Guidelines on the Protection of Privacy and Trans-border flows of Personal Data*. These guidelines were formalized in 1981 by the *Convention for Protection of Individuals with regard to Automatic Processing of Personal Data*, also known as the Treaty of Strasbourg.

When development of both international trade and the need for protection increased, the need for harmonization of European privacy law was felt. In 1995 this resulted in the *Data Protection Directive 95/46/EC*.

The *Charter of Fundamental Rights of the European Union* (the 'Charter', proclaimed in December 2002) included the general principles set out in the ECHR. The Charter explicitly refers to both the protection of privacy and the protection of personal data as a fundamental **right**:

Article 7 - Respect for private and family life
1. Everyone has the right to respect for his private and family life, his home and his correspondence.

Article 8 - Protection of personal data
1. Everyone has the right to the protection of personal data concerning him or her.
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
3. Compliance with these rules shall be subject to control by an independent authority.

Source: Charter of Fundamental Rights of the European Union.

While the progress in data processing increased every year, international trade was hindered by differing laws. The rules and regulations in the member states, although based on directive 95/46/EC, were still quite diverse. After years of discussion, the GDPR was published on 25 May 2016. The GDPR applies as law in all countries of the EEA as of 25 May 2018. The Regulation repeals Directive 95/46/EC. This means that all national law based on this Directive is replaced by the GDPR.

According to GDPR Article 94(2) 'references to the repealed Directive shall be construed as references to this Regulation. References to the Working Party on the Protection of Individuals with regard to the Processing of Personal Data established by Article 29 of Directive 95/46/EC shall be regarded as references to the European Data Protection Board established by [the GDPR]. Article 94 makes clear that, even when member states need more time to update national law that somehow complements law based on Directive 95/46/EC, there can be no confusion on which law applies.

1.1.1 Data Protection history in 'birds view'

Year	Name	Short Name
1948	Universal Declaration of Human Rights	UHDR
1950	European Convention on Human Rights	ECHR
1981	Convention for Protection of Individuals with regard to Automatic Processing of Personal Data	ETS 108 = EU Treaty of Strasbourg
1995	Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data	'Privacy Directive' (repealed 25/5/2018)
2002	Charter of Fundamental Rights of the European Union	'EU Charter'
2016	General Data Protection Regulation (EU) 2016/679	'GDPR' (applicable law since 25/5/2018)
2016	Directive 2016/680 (police and judicial cooperation in criminal matters)	
2016	Directive 2016/681 (on the use of passenger name record (PNR) data)	

1.1.2 Regulation versus Directive

Unlike a Directive, which must be assimilated into each member state's national law, a Regulation is binding and directly applicable to all member states. The GDPR is 'Text with EEA Relevance', which means it applies to all countries within the European Economic Area (EEA). These are all EU member states, Iceland, Liechtenstein and Norway.

1.2 Material and territorial scope of the GDPR

1.2.1 Material scope

This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.

Source: General Data Protection Regulation (EU) 2016/679; article 2(1)

The GDPR applies to personal data in structured form, from fully automated database systems down to paper-based files like the classic medical files still used in some hospitals.

There are some exceptions. Instead of the GDPR, Directive 2016/680, which is national law based on this directive, applies to activities in relation to common foreign and security policy, processing by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.

The GDPR also does not apply to the processing of personal data by a natural person '**in the course of a purely personal or household activity**'. Recital (18) details this as 'activities with no connection to professional or commercial activity, such as personal correspondence and an address book that is kept for that purpose, or social networking and online activities within that context'.

1.2.2 Territorial scope

1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.
2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:
    a. the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or
    b. the monitoring of their behavior as far as their behavior takes place within the Union.

Source: General Data Protection Regulation (EU) 2016/679; article 3

Any processing of personal data in the context of the activities of an establishment of a controller or a processor in the European Union should be carried out in accordance with the GDPR, regardless of where in the world the actual processing takes place.

The GDPR also applies to processing related to trade ('the offering of goods or services') and 'monitoring of behavior' of persons who are in the European Union (recital (23)). This has far reaching consequences. For example, a Canadian company is processing personal data of an Argentinean citizen for an online purchase. If this Argentinian citizen happens to be visiting Paris (France) at the time of the purchase and the Canadian company is aware that it is offering goods or

services to the European Union (because they send the goods to Europe, for instance), this processing is subject to the GDPR.

In addition, the GDPR applies to processing of personal data by a controller **not** established in the EEA, but 'in a place where Member State law applies by virtue of public international law'. Recital (25) gives the example of a Member State's diplomatic mission or consulate.

The GDPR also applies to processing aboard of ships registered in an EU member state, regardless of wherever in the world the ship actually is.

1.3 Definitions

In the first few recitals of the GDPR, its definition of privacy is explicitly linked to the Charter of Fundamental Rights of the European Union.

1. The protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8(1) of the Charter of Fundamental Rights of the European Union (the 'Charter') and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU) provide that everyone has the right to the protection of personal data concerning him or her.
2. The principles of, and rules on the protection of natural persons with regard to the processing of their personal data should, whatever their nationality or residence, respect their fundamental rights and freedoms, in particular their right to the protection of personal data. (…)

Source: General Data Protection Regulation (EU) 2016/679; recitals (1) and (2)

According to this, the [right to] protection of personal data is a means to protect fundamental rights and freedoms of people, among them their privacy.

1.3.1 Privacy

According to the above, privacy is defined as **the right to respect for a person's private and family life, his or her home and correspondence**.

1.3.2 Data Protection

From the former paragraphs, we can conclude that the GDPR concerns the protection of personal data, not all data. Article 4 of the GDPR defines exactly what data are included in the definition.

1.3.3 Personal Data

Article 4(1) of the GDPR defines personal data as:

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

Source: General Data Protection Regulation (EU) 2016/679; Article 4(1)

Any information may be taken literally. It includes 'objective' information such as things that can be measured, for example blood type, shoe size or the amount of alcohol in one's blood. It also includes 'subjective' information, such as opinions about a person (for example, 'John is a good

coach'). For information to be 'personal data', it does not have to be true or proven. Lies or incorrect data about a person are still 'personal data'.

The concept of 'personal data' is not limited to information that might be considered harmful to the individual's private and family life. The medium on which the information is contained is also irrelevant. The concept of personal data includes information available in whatever form: text, figures, graphics, photographs, video, acoustic, or any other possible form.

1.3.4 Natural person

Legally, a 'natural person' is a human being, an individual capable of assuming obligations and capable of holding rights. Therefore, the GDPR does not apply to deceased persons (see recital (27)). Member states, however, may provide for rules regarding the processing of personal data of deceased persons.

1.3.5 Direct, indirect, pseudonymized personal data

In practice, we distinguish three types of personal data.

1.3.5.1 Direct personal data

Direct personal data are data that can be attributed directly to a specific data subject without the use of additional information. For instance, the data subject's photo, DNA, fingerprints. Names can be direct personal data if it is a very unique one. Most names are not unique and are usually not direct personal data. A unique title, such as 'the current prime minister of France', is also a direct reference to an individual, and thus direct personal data.

1.3.5.2 Indirect personal data

Indirect personal data are data that can be, or could be in the future, linked to a specific data subject using additional information. For example, the number plate of a car is indirect personal data, because it is possible to trace the car to its owner using additional information (in this case the information in a database were the number plates are related to the owners of the cars). The same is true for unique numbers assigned to people by the government (social security number) or by one's ISP (IP-address), which can be linked to a unique individual. The fact that not every controller is able to trace a license plate, social security number or IP-address to the associated individual, is not important. The fact that it is in theory possible to identify a person makes it (indirect) personal data.

Names are indirect personal data where the name is common enough not to point to a specific person. To distinguish 'James Williams' from other individuals by that name, additional information such as residence and date of birth are needed.

1.3.5.3 Pseudonymized personal data

Data pseudonymization is the process of disguising identities. The aim of such a process is to be able to collect additional data relating to the same individual without having to know his or her identity. An example might be a camera registering how many unique cars pass a bridge in a road. The license plate number is indirect personal data. The controller would then replace each license plate number with a unique key or pseudonym, keeping a separate table linking each key to the corresponding license plate. The controller might then send this pseudonymized data to a processor, keeping the key in a safe place.

Pseudonymized data are a kind of indirect personal data, where the additional data needed to identify the data subjects ('the key') is only available to the controller. The process is reversible as long as the key exists. Consequently, pseudonymized data on a person is considered personal data, because identification is still technically possible.

Anonymization means that no information from which the person to whom the data relates, can be identified in any way. Anonymized data on a person is **no longer** considered personal data. Pseudonymized data can be anonymized by destroying the key.

For example, for research on health and eating habits a selected group of data subjects is called. Names, telephone numbers and other data of the data subjects are known and kept in a database, for which the data subjects gave their permission. The data subjects are called multiple times during the research. Once the research period is over, all identifiable data are erased after gathering the information needed for the research. This means that the data can no longer be linked to the specific data subjects, because no key exists. Only more general personal data like gender and age category are linked to the data about health and eating habits. In other words, the data that is left after the research is anonymized.

1.3.5.4 Special personal data

The GDPR distinguishes a number of categories of personal data which need special attention. The categories of special personal data are:

- data revealing racial or ethnic origin
- data revealing political opinions
- data revealing religious or philosophical beliefs
- data revealing trade union membership
- genetic data
- biometric data processed for the purpose of uniquely identifying a natural person
- data concerning health
- data concerning a natural person's sex life or sexual orientation

It is forbidden to process special personal data, except in cases which are explicitly mentioned in article 9 of the GDPR.

1.3.6 Processing

In the GDPR, processing data is always meant as the processing of personal data. The GDPR does not apply to the processing of any other data. Having said that, the definition of processing is very wide:

> 'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction
>
> Source: General Data Protection Regulation (EU) 2016/679; Article 4(1)

In fact, it is hard to think of anything that could be done with personal data, but would not be contained in the definition.

Collecting personal data is processing. Storing personal data is processing. Destroying personal data is also processing. Even making a back-up of a server that is not your own, but contains personal data would be considered a kind of storage, which is included in the definition.

1.4 Roles, Responsibilities, Stakeholders

1.4.1 Controller

'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data

Source: General Data Protection Regulation (EU) 2016/679; Article 4(7)

The controller is the natural or legal person responsible for the **determination of the purposes and means of the processing**.

1. Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organizational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.
2. Where proportionate in relation to processing activities, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller.

Source: General Data Protection Regulation (EU) 2016/679; Article 24

In other words, the responsibility and role of the controller is to implement appropriate technical and organizational measures to comply with the GDPR, including 'appropriate data protection policies'.

Article 24(1) indicates that the level of the technical measures needed can vary according to the specific situation and the level of risks to the natural persons involved.

For instance, the invitation to the summer barbecue of the hockey club, though processing of personal data, probably does not need the same level of data security that an invitation to a group of people suffering from a chronic illness does. See also § 1.3.5.4: Special personal data.

Note that the role of the controller is not just about technical implementation of appropriate procedures. The controller is responsible, and must be able to demonstrate, that processing is performed in accordance with the GDPR.

1.4.2 Processor

'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller

Source: General Data Protection Regulation (EU) 2016/679; Article 4(8)

A processor may sometimes be referred to as 'data processor'. The definition indicates that a processor always acts 'on behalf of the controller', and that the processor must comply with the instructions of the controller. The instructions may be written in a contract. The controller-processor contract is discussed in § 8.2: Written Contracts Between the Controller and the Processor.

1.4.3 Data Protection Officer (DPO)

Controllers and processors may, and in the cases cited below **must**, appoint a Data Protection Officer (DPO). The DPO is a person who is formally tasked with ensuring that the organization is aware of, and complies with, its data protection responsibilities and obligations according to the GDPR and Member State law.

The controller and the processor shall designate a data protection officer in any case where:
(a) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity
(b) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale or
(c) the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10

Source: General Data Protection Regulation (EU) 2016/679; Article 37(1)

Organizations that are not required to appoint a DPO are free to do so of their own volition. If an organization voluntarily appoints a DPO, the DPO is held to the GDPR standards. Whenever a DPO is appointed, the organization must communicate this to the relevant supervisory authority and publish the details of the DPO, so that data subjects may reach the DPO. According to recital (97) the DPO should be 'a person with expert knowledge of data protection law and practices'.

Article 38 of the GDPR explicitly requires the controller and processor to ensure that the DPO is involved properly and in a timely manner in all issues which relate to the protection of personal data. They have the obligation to support the DPO in performing his tasks by providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain his or her expert knowledge. The DPO has an **independent** position and is protected by the GDPR:

The controller and processor shall ensure that the data protection officer does not receive any instructions regarding the exercise of those tasks. He or she shall not be dismissed or penalized by the controller or the processor for performing his tasks. The data protection officer shall directly report to the highest management level of the controller or the processor.

Source: General Data Protection Regulation (EU) 2016/679; Article 38(3)

1.4.3.1 Tasks of the DPO

The data protection officer shall have at least the following tasks:
(a) to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions;
(b) to monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;
(c) to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35;
(d) to cooperate with the supervisory authority;
(e) to act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter.

Source: General Data Protection Regulation (EU) 2016/679; Article 39(1)

1.4.4 Recipient

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

Source: General Data Protection Regulation (EU) 2016/679; Article 4(9)

The definition mainly tells us what the recipient is **not**. The recipient is an important stakeholder, being the one to whom personal data or results of processing of personal data are disclosed. In particular where the recipient is outside of the EEA, and even more if the recipient is a Government institution outside the EEA, there are strict rules, which will be discussed later. See § 7.4: Cross-Border Data Transfer.

1.4.5 Third party

'third party' means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorized to process personal data;

Source: General Data Protection Regulation (EU) 2016/679; Article 4(10)

A third party is either 'a natural or legal person, public authority, agency or body'. In any case it is not the data subject, neither the controller nor processor, nor 'persons who, under the direct authority of the controller or processor, are authorized to process personal data'. Then what is a third party?

In principle, a third party is a person or organization with no specific legitimate grounds or authorization to process personal data. An example is an accountant, who in the execution of his duties might unintentionally see personal data. Or a systems manager checking whether the back-up of personal data has been successful and happens to see some names and other personal data.

A third party that receives personal data, either lawfully or unlawfully, is by definition processing personal data. When the processing is not executed under the direct authority of the controller, this 'third party' will, in principle, be regarded as a new controller.

2 Processing of Personal Data

According to the definition of processing, any operation on personal data is contained in the definition of processing. Chapter II of the GDPR (articles 5 through 11) details the data processing principles.

2.1 Data Processing Principles

Processing of personal data always needs to comply with the principles relating to processing of personal data. These principles are:

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimization
- Accuracy
- Storage limitation
- Integrity and confidentiality
- Accountability

2.1.1 Lawfulness, Fairness and Transparency

Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject. The data subject may ask how their data are processed, if it is not clear to them.

2.1.2 Purpose Limitation

Personal data shall be collected for specified, explicit and legitimate purposes and **not further processed** in a manner that is incompatible with those purposes.

Further processing is permitted for:

- archiving purposes in the public interest
- scientific or historical research
- statistical purposes

provided that, in accordance with the GDPR, the appropriate safeguards for the rights and freedoms of the data subject are in place.

2.1.3 Data Minimization

Personal data shall be adequate, relevant and **limited to what is necessary** in relation to the purposes for which they are processed.

2.1.4 Accuracy

Personal data shall be accurate and, where necessary, kept up to date: Every reasonable step should be taken to ensure that personal data which are inaccurate are rectified or deleted.

2.1.5 Storage Limitation

Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; etc.

2.1.6 Integrity and Confidentiality

Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures.

2.1.7 Accountability

The controller is accountable for the data processing. That means that the controller is responsible for compliance with the principles stated above, together with the processor. The controller must also be able to demonstrate compliance with the data processing principles.

3 Legitimate Grounds and Purpose Limitation

3.1 Legitimate Grounds for Processing

According to GDPR art. 6.1, processing shall be lawful only if and to the extent that at least one of the following legitimate grounds for processing applies:

- The data subject has given **consent** to the processing of his or her personal data for one or more specific purposes
- Processing is **necessary for the performance of a contract** to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract
- Processing is necessary for **compliance with a legal obligation** to which the controller is subject
- The processing is necessary in order to **protect a vital interest** of the data subject or of another natural person
- The processing is necessary for the performance of a task carried out in the **public interest** or in the exercise of **official authority** vested in the controller
- The processing is necessary for the purposes of the **legitimate interests** pursued by the controller or by a third party
    - **except** where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child

This list of legitimate grounds is exhaustive. There are no other legitimate grounds for processing of personal data under the GDPR.

3.1.1 Purpose Limitation and Purpose Specification

Purpose specification as a term is not explicitly defined in the GDPR. However, in April 2013 the Article 29 Working Party (WP29), composed of representatives of the European supervisory authorities, the European Data Protection Supervisor and the European Commission, published an opinion on the purpose limitation principle when processing personal data. The WP29's opinions provide authoritative guidance on EU data protection rules.

From 25 May 2018 the Article 29 Working Party is succeeded by the European Data Protection Board (EDPB) as defined in GDPR article 68. In its first meeting the EDPB endorsed the guidelines and other documents on the GDPR published by WP29 to ascertain continuity. Many of the guidelines and opinions WP29 published before May 2018 are incorporated or referenced in the GDPR.

Personal data must be collected for specified purposes. The controller must therefore carefully consider what purpose or purposes the personal data will be used for, and must not collect personal data which are not necessary, adequate or relevant for the purpose or purposes which are intended to be served.

Source: WP29 opinion on purpose limitation, § III.1.1. (Purposes must be specified) (as viewed on 24 July 2019)

Article 5(1)(b) of the GDPR requires that 'personal data shall be collected for specified, explicit and legitimate purposes (…)'. Let us look at the elements of that sentence:

3.1.1.1 Specified

In order to determine whether data processing complies with the law, and to establish what data protection safeguards should be applied, it is a necessary precondition to identify the specific purpose(s) for which the collection of personal data is required. Purpose specification thus sets limits on the purposes for which controllers may use the personal data collected, and also helps establish the necessary data protection safeguards.

Purpose specification requires an internal assessment carried out by the data controller and is a necessary condition for accountability. It is a key first step that a controller should follow to ensure compliance with applicable data protection law. The controller must identify what the purposes are, and must also document, and be able to demonstrate, that it has carried out this internal assessment.

Source: WP29 opinion on purpose limitation (as viewed on 24 July 2019)

Because collecting personal data is processing personal data, the purpose must be specified **prior** to the collection of personal data.

The purpose specification must be detailed enough to determine what kind of processing is and is not included within the specified purpose. A purpose that is vague or general, such as 'improving users' experience', 'marketing purposes', or 'future research' will, without more detail, usually not meet the criteria of being ‘specific’. A message to the data subject that ‘browsing information is processed in order to present advertisements relating to their interests’ would relate exactly what the purpose is and how it is achieved.

3.1.1.2 Explicit

Personal data must be collected for explicit purposes. The purposes of collection must not only be specified in the minds of the persons responsible for data collection. They must also be made explicit. In other words, they must be clearly revealed, explained or expressed in some intelligible form. It follows from the previous analysis that this should happen no later than the time when the collection of personal data occurs.

The ultimate objective of this requirement is to ensure that the purposes are specified without vagueness or ambiguity as to their meaning or intent. What is meant must be clear and should leave no doubt or difficulty in understanding. The specification of the purposes must, in particular, be expressed in such a way so as to be understood in the same way not only by the controller (including all relevant staff) and any third-party processors, but also by the data protection authorities and the data subjects concerned. Particular care should be taken to ensure that any specification of the purpose is sufficiently clear to all involved, irrespective of their different cultural/linguistic backgrounds, level of understanding or special needs.

Source: WP29 opinion on purpose limitation (as viewed on 24 July 2019)

Explicit purpose specification makes transparent how controllers intend to use the personal data collected. It helps all those parties that are processing data on behalf of the controller, as well as data subjects, supervisory authorities and other stakeholders, to have a common understanding of how the data can be used. This, in turn, reduces the risk that the data subjects' expectations will differ from the expectations of the controller.

3.1.1.3 Legitimate

The requirement of legitimacy means that the purposes of data processing must be 'in accordance with the law' in the broadest sense (GDPR Article 6(3)). This includes all forms of written and common law, primary and secondary legislation, municipal decrees, judicial precedents, constitutional principles, fundamental rights, other legal principles, as well as jurisprudence, as such 'law' would be interpreted and considered by competent courts.

In addition to any other law, GDPR Article 6(1) always applies to personal data processing. In order for the processing to be lawful, the processing must **at all times** be based on at least one of the six legitimate grounds for processing (see § 3.1: legal grounds).

3.1.2 Proportionality and subsidiarity

3. Under the principle of subsidiarity, in areas which do not fall within its exclusive competence, the Union shall act only if and in so far as the objectives of the proposed action cannot be sufficiently achieved by the Member States, either at central level or at regional and local level, but can rather, by reason of the scale or effects of the proposed action, be better achieved at Union level. (…)
4. Under the principle of proportionality, the content and form of Union action shall not exceed what is necessary to achieve the objectives of the Treaties.

Source: Treaty on the Functioning of the European Union art. 5

This seems far away of the practice of protecting privacy and personal data, but it is not. These principles form a red thread throughout the GDPR, down to the practical level.

3.1.2.1 Subsidiarity

In addition to in this treaty, subsidiarity is also found in the general rule that requires that personal data can only be processed if there is **no other means to achieve the purposes**. Five of the six legal grounds for processing require that the processing is absolutely necessary. When there are other means to achieve the purposes, it is hard to maintain that the processing of personal data is necessary.

For example, suppose one wants to find out how many people walk a shopping street on an average Saturday afternoon. For this purpose, it is not necessary to identify the individuals. It would be possible to count individuals with a smartphone by using the signal of their smartphone (a MAC-address, for instance). However, since a MAC-address could be traced to the individual who owns the smartphone this signal is considered personal data. There are definitely other ways to count the number of people passing a street without using personal data. One could for instance post observers and simply count individuals. The subsidiarity principle in the GDPR would mean that using the MAC-address is an illegal use of personal data, because your interest to count the number of visitors is overridden by the fundamental right to privacy of the visitors. You will have to use a method which keeps the visitors anonymous and does not collect direct or indirect personal data.

3.1.2.2 Proportionality

The principle of proportionality is closely related to subsidiarity. Proportionality requires that any action by the EU should not go beyond what is necessary to achieve the objectives of the Treaties. When applied to personal data processing, this translates as no more data than strictly necessary should be collected. We find this at the practical level with the principle of data minimization: ‘personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed’. This seems obvious, but we all know examples where more information is gathered than strictly necessary for the purpose specified. For example, when a web shop collects data on gender in their shipping address form, while that is not necessary for sending their product to the customer.

4 Rights of Data Subjects

From the history of privacy and data protection we have seen that the fundamental rights of the data subject are considered of the utmost importance. The GDPR states that processing of personal data is prohibited, except when a number of requirements are met. There must be a lawful reason for the processing. The purpose of the processing must be clearly specified. And even then, if there are other means than processing of personal data to achieve the specified purpose, those other means should be used.

Even when all requirements are met, the controller must at all times balance the fundamental rights of the data subject with the purposes of the processing. No wonder that a relatively large section of the GDPR is dedicated to the rights of a data subject.

4.1 Transparent Information, Communication and Modalities

A basic idea in the GDPR is that a data subject must be **informed** whenever his or her personal data are processed. If processing is based on consent, the data subject should know and understand what he or she is consenting to ('informed consent').

When processing is based on one or more of the other legitimate grounds for processing, the data subject should still be informed about which personal data are processed, to what purpose and who is responsible. And by 'know' and by 'be informed' the GDPR explicitly means 'be aware of' and 'understand it'.

> The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.
>
> Source: General Data Protection Regulation (EU) 2016/679; Article 12(1)

The articles cited above are discussed in the following paragraphs. They detail the various rights data subjects have when their personal data are processed.

> The controller shall facilitate the exercise of data subject rights under Articles 15 to 22. In the cases referred to in Article 11(2), the controller shall not refuse to act on the request of the data subject for exercising his or her rights under Articles 15 to 22, unless the controller demonstrates that it is not in a position to identify the data subject.
>
> Source: General Data Protection Regulation (EU) 2016/679; Article 12(2)

There are two important exemptions to acting on the request of a data subject.

- First of all, controllers may, and often must, require data subjects to provide proof of identity. This helps to limit the risk that third parties gain unlawful access to personal data.
- Second, the controller is exempt from its obligation to comply with certain rights of data subjects if it cannot identify which data in its possession relates to the relevant data subject.

The second paragraph of article 12 is at least as important. It is great to have a right to something, but not everybody feels sufficiently empowered to exercise their rights when some company or governmental institution tells them that processing of their data is intended.

According to article 12(2), a controller planning processing must inform the data subjects about the rights they have, and assist them in exercising those rights. The information about the intended processing mentioned before and the assistance to the data subject shall be provided free of charge. When ignoring this obligation, a controller risks huge fines (see § 7.3.3).

4.2 Information on and Access to Personal Data

In addition to the information referred to in paragraph 1, the controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing:

Source: General Data Protection Regulation (EU) 2016/679; Article 13(2)

4.2.1 Information to be provided to the data subject in any case

There are slight differences in what information must be provided to the data subject, dependent on whether the personal data to be processed is being collected from the data subject (GDPR art. 13) or from other sources (GDPR art. 14).

In all cases the controller must provide:

- the identity and the contact details of the controller and its representative, where applicable
- the contact details of the data protection officer (DPO), where applicable
- the purposes of the processing for which the personal data are intended
- the legal basis for the processing
- the period for which the personal data will be stored (retention period), or if that is not possible, the criteria used to determine that period.
- the existence of the right to request from the controller
    - access to their personal data
    - rectification or erasure of their personal data
    - restriction of processing
    - object to processing as well as the right to data portability
- where the processing is based on consent, the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal
- the right to lodge a complaint with a supervisory authority

In addition, if the legitimate ground of the processing is based on 'the legitimate interests pursued by the controller or by a third party':

- the legitimate interests pursued by the controller or by a third party

4.2.2 Information to be provided to the data subject when transferring personal data

If the controller intends to transfer personal data to a third country or international organization, additional details are to be provided:

- the recipients or categories of recipients of the personal data

And if this transfer is to a recipient outside the EEA or an international organization:

- the fact that the controller intends to transfer personal data to a recipient in a third country or international organization
- the existence of an adequacy decision by the Commission, or if not, which appropriate safeguards are in place

4.2.3 Additional information to be provided when personal data are not obtained from the data subject directly

When the personal data have not been obtained from the data subject directly, some additional information shall be provided:

- the categories of personal data concerned
- from which source the personal data originate, and if applicable, whether it came from publicly accessible sources

4.2.4 Timing of the information to be provided

The controller shall provide the information referred to above:

- within a reasonable period after obtaining the personal data, but at the latest within one month
- with regard to the specific circumstances in which the personal data are processed
- if the personal data are to be used for communication with the data subject, at the latest at the time of the first communication to that data subject or,
- if a disclosure to another recipient is envisaged, at the latest when the personal data are first disclosed

There are a few extra obligations for special cases, and a few exceptions to these rules. See GDPR article 15.4.

4.3 Right of Access (Inspection) by the Data Subject

The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data (…)

Source: General Data Protection Regulation (EU) 2016/679; Article 15(1).

Notwithstanding the rules about being informed, as detailed above, a data subject has at any time the right to obtain information from the controller on whether personal data concerning him or her are being processed.

And if data are being processed, the controller is obliged to give the information mentioned above and a copy of the data being processed for free. Additional copies of the data may be charged to the data subject, but only at a reasonable price based on administrative costs.

An important restriction on the right of the data subject to obtain a copy of the personal data processed or to be processed is that the request may not adversely affect the rights and freedoms of others.

4.4 Rectification and Erasure

4.4.1 Right to rectification

Of course, when a data subject receives a copy of the personal data on him or her from the controller, the data subject may find that the data are incorrect. In that case the data subject can demand rectification:

> The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.
>
> Source: General Data Protection Regulation (EU) 2016/679; Article 16.

4.4.2 Right to erasure ('right to be forgotten')

Data subjects have the right to have their data 'erased' in certain cases. Such a case will usually be when the processing fails to satisfy the requirements of the GDPR. The right can be exercised against controllers, who must respond without undue delay (and in any event within one month, although this can be extended in difficult cases)

> The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay (…)
>
> Source: General Data Protection Regulation (EU) 2016/679; Article 17.

Grounds to have personal data erased might be:

- The data are no longer necessary for the intended purposes of processing
- Withdrawal of consent
- The data were collected for an offer of information services directly to a child below the age of 16 years
- Objections to the processing (see below)
- Unlawful processing
- Compliance with Union or Member State law which applies to the controller

The right to erasure on these grounds only has effect when the specific ground was the only legitimate ground for processing. For example, data subjects demanding that the government erases the personal data necessary to calculate their income tax because they no longer consent will not succeed, because in that case 'consent' was not the ground for legitimate processing.

4.4.3 Right to restriction of processing

Data subjects have the right to restrict the controller in processing their data in certain cases. Grounds to have processing restricted might be:

- The accuracy of the data is contested by the data subject
    - processing of the personal data is restricted for the time it takes to verify the claim and rectify the data
- the processing is unlawful and the data subject opposes the erasure of the personal data
- the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defense of legal claims

- the data subject has objected to processing pursuant to Article 21(1) (the right to object) pending the verification whether the legitimate grounds of the controller override those of the data subject

What does it mean when processing has been restricted?

Where processing has been restricted under paragraph 1, such personal data shall, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defense of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or of a Member State.

Source: General Data Protection Regulation (EU) 2016/679; Article 18(2).

The controller must notify the data subject before lifting a restriction.

4.4.4 Notification obligation (rectification / erasure / restriction of processing)

The controller shall communicate any rectification or erasure of personal data or restriction of processing carried out in accordance with Article 16, Article 17(1) and Article 18 to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The controller shall inform the data subject about those recipients if the data subject requests it.

Source: General Data Protection Regulation (EU) 2016/679; Article 19.

This obligation means that, in addition to implementing systems and procedures for ensuring the data subject's rights, controllers must implement systems and procedures for notifying affected third parties about the exercise of those rights.

Cartoon © Pierre Kroll, derived with authorization from the leaflet 'Take Control of your Personal Data' (2012), ISBN 978-92-79-22654-0, Published by European Commission - Directorate-General for Justice

4.4.5 Right to data portability

The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, (…).

Source: General Data Protection Regulation (EU) 2016/679; Article 20.

If processing is based on consent or on a contract, **and** the processing is carried out by automated means, data subjects have the right to receive the personal data or to transfer their personal data between controllers. The data subjects have the right to move account details from one online platform to another.

This right makes it easier for customers to switch to another online supplier, such as web shops or other online businesses. Setting up a new account should become easier, because the controller must allow account information to be transferred to a competitor.

Note that the right to data portability does **not** apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

4.5 Right to Object and Automated Individual Decision-Making

4.5.1 Right to object

As set out in § 3.1: Legitimate grounds for processing, a controller must have a lawful basis for processing personal data. Nevertheless, where that lawful basis is either 'public interest' or 'legitimate interests' (including profiling), data subjects may have a right to object to such processing.

The GDPR then requires the organization to demonstrate that it either has compelling grounds for continuing the processing, or that the processing is necessary in connection with its legal rights. If it cannot demonstrate that one of these two grounds apply, it must cease that processing activity.

4.5.2 Automated individual decision-making, including profiling

Where personal data are processed for the purposes of direct marketing, the data subject should have the right to object to such processing, including profiling to the extent that it is related to such direct marketing, whether with regard to initial or further processing, at any time and free of charge. That right should be explicitly brought to the attention of the data subject and presented clearly and separately from any other information.

Source: General Data Protection Regulation (EU) 2016/679; Recital (70).

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

Article 22.1 adds to this that the data subject has the right not to be subject to a decision based solely on automated processing. This paragraph, however, does not apply if the decision is based on the data subject's explicit and informed consent.

4.6 Right to Lodge a Complaint with a Supervisory Authority

Without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a supervisory authority, in particular in the Member State of his or her habitual residence, place of work or place of the alleged infringement if the data subject considers that the processing of personal data relating to him or her infringes this Regulation.

Source: General Data Protection Regulation (EU) 2016/679; Article 77(1).

Data subjects have the right to lodge a complaint concerning the processing of his or her personal data with the supervisory authority in the member state where they live, or in the member state where the alleged infringement occurred. The GDPR contains rules to make sure that the right of the data subject to an effective judicial remedy is upheld by all parties, including controller or controllers, processor or processors and supervising authority or supervisory authorities involved.

5 Personal Data Breaches and Related Procedures

5.1 The Concept of Personal Data Breach

'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed;

Source: General Data Protection Regulation (EU) 2016/679; Article 4(12).

In the GDPR, a personal data breach is **always** a security incident. It is not just a vulnerability (security risk) or a security threat. The security manager's nightmare has just come true and someone has had access to data.

For a personal data breach, the security incident must have led to a situation where personal data has or may have been processed unlawfully. This means that not every security incident is a personal data breach. Remember that destroying, storing and copying are also considered processing.

Articles on the subject of personal data breaches often give examples with scenarios that include malicious or benign hacking and third parties getting unauthorized access to personal data. However, the GDPR definition of personal data breach is far broader.

A fire in a data center could destroy personal data stored there. That would make it both a security incident, because data are no longer available, and a personal data breach, because personal data was processed, in this case destroyed, without authorization.

In a similar way, when a processor accidentally deletes a set of personal data, the processor is in violation of GDPR article 29, which makes the processing unlawful:

The processor and any person acting under the authority of the controller or of the processor, who has access to personal data, shall not process those data except on instructions from the controller, unless required to do so by Union or Member State law.
Source: General Data Protection Regulation (EU) 2016/679; Article 29.

In literature, the term 'data breach' is often used where 'personal data breach' is meant. The difference is that a 'data breach' can, depending on the context, also refer to a breach where commercial or other company data are compromised. A personal data breach is always a data breach. A data breach is only a personal data breach when personal data are involved.

5.2 Procedures on how to Act when a Personal Data Breach Occurs

Article 32 of the GDPR requires **both** controllers and processors to 'implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk'.

Internationally accepted information security standards such as ISO/IEC 27001 will usually be in place. Those standards have procedures to handle an incident with the aim of repairing the damage and preventing recurrence of the incident.

A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorized reversal of pseudonymization, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned.

Source: General Data Protection Regulation (EU) 2016/679; Recital (85).

5.2.1 Notification of a personal data breach to the supervisory authority

In the event of a personal data breach, data controllers must notify the **supervisory authority**. Notice must be provided 'without undue delay and, where feasible, not later than 72 hours after having become aware of it.'

When the personal data breach is reported later than 72 hours after noticing the personal data breach, a good reason for the delay must be sent with the notification.

Article 33(1) contains an important exception to the data breach notification requirement. Notice is **not** required if 'the personal data breach is unlikely to result in a risk for the rights and freedoms of natural persons.'

5.2.2 Notification of a personal data breach to the controller

When a data processor experiences a personal data breach, they must notify the **controller** 'without undue delay after becoming aware of a personal data breach'.

The processor has no other notification or reporting obligation under the GDPR. All other notification and reporting must be done by the controller.

5.2.3 Notification of a personal data breach to the data subject

If the controller determines that the personal data breach 'is likely to result in a high risk to the rights and freedoms of individuals', they must communicate information regarding the personal data breach to the affected **data subjects**. This must be done, according to article 34, 'without undue delay'.

There are three exceptions to the additional requirement to notify data subjects. Notification to the data subject is **not** obligatory in the following circumstances:

- when the data are unreadable
- when other measures are taken to minimize the risk
- when notifying is a disproportionate effort

5.2.3.1 Encryption and other protection measures

The controller has 'implemented appropriate technical and organizational protection measures' that 'render the data unintelligible to any person who is not authorized to access it, such as encryption'.

5.2.3.2 Mitigating measures

The controller takes actions after the personal data breach to 'ensure that the high risk for the rights and freedoms of data subjects' is unlikely to materialize.

5.2.3.3 Disproportionate effort

When notification to each data subject would 'involve disproportionate effort'. In this case, alternative communication measures may be used, such as a notification on the company website.

5.3 Categories of Personal Data Breaches

Three categories of personal data breach can be distinguished. Personal data breaches which:

- are **unlikely** to result in a risk for the rights and freedoms of natural persons;
  - notification of the breach is not obligatory
- **may** result in physical, material or non-material damage to natural persons
  - notification to the supervisory authority is obligatory
- are **likely** to result in a high risk to the rights and freedoms of individuals
  - notification to the supervisory authority
  - notification to the data subjects is obligatory, if possible

Organizing Data Protection

6 Importance of Data Protection for the Organization

Almost all organizations process personal data. For an organization processing personal data, data protection is not just 'a requirement of the law' or 'important to avoid fines'. The reputation of the organization is at stake.

Processing personal data in a professional way means quality assurance, security management and governance.

The following paragraphs outline the requirements for lawful processing of personal data.

6.1 Requirements for Compliance with the GDPR

Under the GDPR, processing of personal data is prohibited, unless the requirements of the GDPR are met. The following requirements must be met.

6.1.1 Principles relating to processing of personal data are met

In particular, the data protection principles set out in § 2.1 must have been satisfied. The purpose must be clear, detailed and specified, and at least one of the six possible 'legal grounds for processing' must apply. The rights of the data subject must be guaranteed and adequate data protection measures must be in place.

6.1.2 Legal structure

The GDPR requires controllers, processors and in fact anyone who processes personal data to comply with the GDPR. The controller, as the one determining the purposes and means of processing, is obliged to implement appropriate technical and organizational measures to ensure that processing is performed in accordance with the GDPR.

As we have seen in §1.4.1, the controller is **also** accountable for having these 'appropriate measures' implemented, by the processor, to make sure that the processing takes place in compliance with the data processing principles laid down in the regulation (see also § 2.1). As a consequence, a processor cannot outsource part of the processing to a sub-processor without prior specific or general written authorization of the controller.

The processor only processes the personal data based on documented instructions from the controller. It is obligatory to have a binding legal contract in place. It binds the processor to the controller and sets out:

- the subject matter of the processing
- the duration of the processing
- the nature and purpose of the processing, as set out by the controller
- the type of personal data involved
- categories of data subjects
- the obligations and rights of the controller

In order to be able to **demonstrate compliance** to the requirements, the controller and the processor must document how they comply. Some of the documents showing compliance are obligatory and in a prescribed format. The other documents are needed when something goes wrong or when there is an additional reason for the supervisory authority to inspect compliance with the Regulation.

6.1.3 Impact assessment

Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.

Source: General Data Protection Regulation (EU) 2016/679; article 35(1)

Published guidelines are available indicating in which cases of processing a data protection impact assessment (DPIA) must be performed.

Instead of DPIA, often the term PIA (privacy impact assessment) is used. In the context of the GDPR, the two terms describe the same assessment. What a DPIA comprises and what its objectives are, is discussed in §8.3.

6.1.4 Controller-processor contract

When the controller wants to outsource part of the processing operation to another party, which then becomes a processor, a binding legal contract must be in place. The details of such a contract are described in §8.2.

6.1.5 Prior consultation

The controller shall consult the supervisory authority prior to processing where a data protection impact assessment under Article 35 indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk.

Source: General Data Protection Regulation (EU) 2016/679; article 36(1).

In contrast to the requirements in directive 95/46/EC, the GDPR states that the controller does not have the obligation of prior consultation with a supervisory authority for all processing operations. Prior consultation with the supervisory authority is only necessary if a DPIA indicates a **high risk** to the privacy or rights and freedoms of natural persons.

6.2 Required Types of Administration

6.2.1 Record of processing activities

Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility.

Source: General Data Protection Regulation (EU) 2016/679; article 30(1).

The **controller's record** shall contain:

(a) the name & contact details of the controller(s) or their representatives and data protection officer
(b) the purposes of the processing
(c) a description of the categories of data subjects and categories of personal data
(d) the categories of recipients to whom the personal data have been or will be disclosed, including recipients in third countries or international organizations
(e) where applicable, the transfers of personal data to a third country or an international organization, including the identification of that country or international organization (…)
(f) where possible, the envisaged time limits for erasure of the different categories of data
(g) where possible, a general description of the technical and organizational security measures

Article 30 requires the controller to keep a 'record of processing activities under its responsibility'.

When a processor performs processing activities on instruction of the controller, the processor also needs to keep records:

> Each processor and, where applicable, the processor's representative shall maintain a record of all categories of processing activities carried out on behalf of a controller, (…)
>
> Source: General Data Protection Regulation (EU) 2016/679; Article 30(2).

The **processor's record** shall contain:

(a) the name and contact details of the processor(s) and of each controller on behalf of which the processor is acting, and, where applicable, of the controller's or the processor's representative, and the data protection officer (DPO)
(b) the categories of processing carried out on behalf of each controller
(c) where applicable, transfers of personal data to a third country or an international organization, including the identification of that third country or international organization (…)
(d) where possible, a general description of the technical and organizational security measures

The records of controllers and processors are not necessarily the same. The controller may use multiple processors. A processor may be under contract with multiple controllers.

There is an **exception** to the obligation for small companies and organizations:

> The obligation to keep records of all processing activities does not apply to organizations or enterprises employing fewer than 250 persons unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data (…) or personal data relating to criminal convictions and offences (…).
>
> Source: General Data Protection Regulation (EU) 2016/679; Article 30(5).

In practice, this exception only helps to a limited extent, since it does not relieve the controller of the obligation to demonstrate compliance.

6.2.2 Record of personal data breaches

The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article.

Source: General Data Protection Regulation (EU) 2016/679; Article 33(5).

The 'facts relating to the personal data breach' are:

- Name and contact details of DPO or other contact of the contact where more information can be obtained
- The nature of the data breach
- The categories and approximate number of data subjects involved
- The categories and approximate number of personal data records affected
- The likely consequences in terms of risk to rights and freedoms of natural persons
- The measures taken or to be taken to address the consequences of the personal data breach

7 Supervisory Authorities

Even before the introduction of the GDPR, a system of closely cooperating 'supervisory authorities' was put in place. Often, they are called 'Data Protection Authority' (DPA) or a translation of that term in the local language.

The establishment of supervisory authorities in Member States, empowered to perform their tasks and exercise their powers with complete independence, is an essential component of the protection of natural persons with regard to the processing of their personal data. Member States should be able to establish more than one supervisory authority, to reflect their constitutional, organizational and administrative structure.

Source: General Data Protection Regulation (EU) 2016/679; recital (117).

EEA member states can establish several supervisory authorities. For example, Germany has a supervisory authority for each of their 16 federal states. However, most EEA member states have a single national supervisory authority.

The independence of the supervisory authorities is an important part of the structure:

1. Each supervisory authority shall act with complete independence in performing its tasks and exercising its powers in accordance with this Regulation.
2. The member or members of each supervisory authority shall, in the performance of their tasks and exercise of their powers in accordance with this Regulation, remain free from external influence, whether direct or indirect, and shall neither seek nor take instructions from anybody.
3. Member or members of each supervisory authority shall refrain from any action incompatible with their duties and shall not, during their term of office, engage in any incompatible occupation, whether gainful or not.
4. Each Member State shall ensure that each supervisory authority is provided with the human, technical and financial resources, premises and infrastructure necessary for the effective performance of its tasks and exercise of its powers, including those to be carried out in the context of mutual assistance, cooperation and participation in the Board.
5. Each Member State shall ensure that each supervisory authority chooses and has its own staff which shall be subject to the exclusive direction of the member or members of the supervisory authority concerned.
6. Each Member State shall ensure that each supervisory authority is subject to financial control which does not affect its independence and that it has separate, public annual budgets, which may be part of the overall state or national budget.

Source: General Data Protection Regulation (EU) 2016/679; article 52).

7.1 General Responsibilities of a Supervisory Authority

The main responsibility of a supervisory authority is to **monitor and enforce** the application of the GDPR, with the aim to **protect** the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union (article 51).

Another important responsibility is to promote public awareness and understanding of the risks, rules, safeguards and rights in relation to processing personal data. Activities addressed specifically to children shall receive extra attention.

The list of tasks detailed in GDPR article 57(1) is long and open-ended, as the last one is 'fulfil any other tasks related to the protection of personal data'.

Below the various tasks are summarized and categorized in groups.

7.1.1 To monitor and enforce the application of the Regulation

The supervisory authority monitors the application of the GDPR.

This can be **preventive**, by monitoring relevant developments or conducting investigations, where they have an impact on the protection of personal data.

It can also be **remedial**, by investigating processing operations, including investigations based on complaints of data subjects, organizations or associations and on information received from another supervisory authority or other public authority.

The supervisory authority can also carry out a periodic review of certifications issued to controllers in accordance with article 42(7).

7.1.2 To advise and promote awareness

In accordance with EEA member state law, the supervisory authority advises the national parliament, the government, and other institutions and bodies relating to the protection of natural persons' rights and freedoms with regard to processing.

The supervisory authority also gives advice on the processing operations, either to promote the awareness of controllers and processors of their obligations under the GDPR or more specific in response to a request for consultation from a controller or in the course of an investigation following a personal data breach notification.

On the other side, upon request, the supervisory authority will also provide information to any data subject concerning the exercise of their rights under the GDPR and, if appropriate, cooperate with the supervisory authorities in other Member States to that end.

7.1.3 To administrate personal data breaches and other infringements

The supervisory authority will keep internal records of infringements of the GDPR and of measures taken in accordance with the powers of the supervisory authority as defined in GDPR article 58 (see §7.3 Powers of the Supervisory Authority in Enforcing the GDPR).

7.1.4 To set standards

The supervisory authority has the responsibility to set standards and guidelines and act as a certifying body.

7.1.4.1 Processing requiring DPIA

The supervisory authority publishes the list of the processing operations which are subject to the requirement of a data protection impact assessment (see §8.3).

7.1.4.2 Codes of conduct and certification

The supervisory authority shall encourage the drawing up of codes of conduct intended to contribute to the proper application of the GDPR. The supervisory authority shall provide an opinion on proposals from associations and bodies to prepare or amend a code of conduct, and approve codes of conduct which provide sufficient safeguards. The supervisory authority will also conduct the accreditation of a body for monitoring codes of conduct as described.

The supervisory authority will encourage the establishment of data protection certification mechanisms and of data protection seals and marks for the purpose of demonstrating compliance with the GDPR of processing operations by controllers and processors, and approve the criteria of certification.

The supervisory authority will also draft and publish the criteria for accreditation of a certification body to monitor this certification mechanism.

7.1.4.3 Standard contractual clauses and binding corporate rules and - contracts

A supervisory authority may adopt standard contractual clauses for the binding contract between controller and processor, and if appropriate (i.e. with prior written authorization of the controller), between processor and sub-processor.

A supervisory authority may also adopt standard contractual clauses for contracts between controllers in the EEA and processors in countries outside the EEA for which no adequacy decision has been implemented (see § 7.4: Cross-Border Data Transfer).

Particularly for multi-national companies and organizations, the supervisory authority can approve binding corporate rules (see § 7.6.3: Binding corporate rules (BCR)).

7.1.5 To cooperate with other supervisory authorities and the EDPS.

In order to contribute to the consistent application of this Regulation throughout the Union, the supervisory authorities shall cooperate with each other and, where relevant, with the Commission, through the consistency mechanism as set out in this Section.

Source: General Data Protection Regulation (EU) 2016/679; article 63.

From the previous paragraphs you might have the idea that the more than fifty supervisory authorities in the roughly thirty EEA countries are independently inventing the same standards at the same time. The opposite is true, however. Through the consistency mechanism, supervisory authorities share information and provide mutual assistance to other supervisory authorities ‘with a view to ensuring the consistency of application and enforcement of the GDPR’.

They also share all relevant information with the European Data Protection Board (also known as the 'Board'), which is composed of the head of one supervisory authority of each member state and of the European Data Protection Supervisor, or their respective representatives.

When a supervisory authority takes a decision that only affects the processing of personal data on its own territory, the consistency mechanism does not apply. However, when a supervisory authority takes a decision, for instance to plan to adopt standards, guidelines, or contractual clauses, it will share this information with the Board. In most cases, the Board will, in close communication with the European Commission see to it that, after necessary discussion and necessary amendments, the proposal grows into a European standard adopted by all supervisory authorities.

In principal, the consistency mechanism is intended to ensure that organizations operating internationally face consistent compliance requirements in the EEA countries where they do business.

7.2 Roles and Responsibilities Related to Personal Data Breaches

When a supervisory authority receives a notification of a personal data breach, they must be able to evaluate a number of important criteria to assess the importance of the personal data breach and

to assess the way data protection was implemented by the controller and the processor or processors.

The assessment of the risks to data subjects and mitigating measures that have already been or must still be taken, is clearly the most immediate. The responsibility of the supervisory authority to enforce the rules of the GDPR follows directly after that.

In principle, the controller is responsible for:

- investigating the personal data breach
- the circumstances that led to it
- the assessment of the risks involved for the data subjects
- taking mitigation measures to minimize the negative consequences to the rights and freedoms of the data subjects and other persons involved

However, a Supervisory authority has been given far-reaching powers to monitor that investigation and to order the controllers and processors involved to take other or extra measures, to bring processing operations in line with the GDPR, and even to restrict or block processing.

7.3 Powers of the Supervisory Authority in Enforcing the GDPR

One of the main responsibilities of a supervisory authority is to **enforce** the application of the GDPR. Beside the advisory powers, a supervisory authority has large investigative and corrective powers to enforce the implementation of the GDPR. This includes, when necessary, giving crippling fines.

In order to ensure consistent monitoring and enforcement of this Regulation throughout the Union, the supervisory authorities should have in each Member State the same tasks and effective powers, including powers of investigation, corrective powers and sanctions, and authorization and advisory powers, in particular in cases of complaints from natural persons, (…).

Source: General Data Protection Regulation (EU) 2016/679; Recital (129).

7.3.1 Investigative powers of the supervisory authority

Article 58(1) of the GDPR grants supervisory authorities quite some investigative powers. They have the power:

(a) to order the controller and the processor, (…) to provide any information it requires for the performance of its tasks
(b) to carry out investigations in the form of data protection audits
(c) to carry out a review on certifications issued (…)
(d) to notify the controller or the processor of an alleged infringement of this Regulation
(e) to obtain, from the controller and the processor, access to all personal data and to all information necessary for the performance of its tasks
(f) to obtain access to any premises of the controller and the processor, including to any data processing equipment and means, in accordance with Union or Member State procedural law

7.3.2 Corrective powers of the supervisory authority

Article 58(2) of the GDPR also grants supervisory authorities far-reaching corrective powers:

(a) to issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of the GDPR
(b) to issue reprimands to a controller or a processor where processing operations have infringed provisions of the GDPR
(c) to order the controller or the processor to comply with the data subject's requests to exercise his or her rights pursuant to the GDPR
(d) to order the controller or processor to bring processing operations into compliance with the provisions of the GDPR (…)
(e) to order the controller to communicate a personal data breach to the data subject
(f) to impose a temporary or definitive limitation including a ban on processing
(g) to order the rectification or erasure of personal data or restriction of processing (…) and the notification of such actions to recipients to whom the personal data have been disclosed (…)
(h) to withdraw a certification or to order the certification body to withdraw a certification issued (…), or to order the certification body not to issue certification (…)
(i) to impose an administrative fine (…), in addition to, or instead of measures referred to in this paragraph, depending on the circumstances of each individual case
(j) to order the suspension of data flows to a recipient in a third country or to an international organization

7.3.3 General conditions for imposing administrative fines

Each supervisory authority shall ensure that the imposition of administrative fines pursuant to this Article in respect of infringements of this Regulation referred to in paragraphs 4, 5 and 6 shall in each individual case be effective, proportionate and dissuasive.

Source: General Data Protection Regulation (EU) 2016/679; article 83(1).

Administrative fines must be proportionate and dissuasive.

7.3.3.1 Proportionate

When a supervisory authority decides to impose an administrative fine, in addition to other measures, they must give due regard to the circumstances.

Criteria for that decision are:

- the nature, gravity and duration of the infringement
- the purpose of the processing
- the number of data subjects affected
- the level of damage caused to them
- the degree of responsibility of controllers and processors
    - considering the technical and organizational measures implemented

Cooperation with the supervisory authority to remedy an infringement and mitigate the possible adverse effects of the infringement will speak in the favor of the controllers and processors.

7.3.3.2 Dissuasive

A fine is also to be dissuasive. Whatever the cost of implementing measures to comply with the GDPR in an organization may cost, no company should want to risk ignoring the rules, because the fines will go far beyond whatever compliance will cost.

Still, the intention is to encourage companies to comply with the GDPR, not to financially destroy them.
There are two categories of fines.

- fines of € 10.000.000 or 2% of the company's worldwide turnover of the preceding financial year, whichever is higher
- fines of € 20.000.000 or 4% of the company's worldwide turnover of the preceding financial year, whichever is higher

For infringements of the **obligations of the controller and processor**, the maximum fine will be of the first category, so € 10.000.000 or 2% of the company's worldwide turnover of the preceding financial year, whichever is higher.

Some categories of infringements will be fined more stringent:

- infringements of the basic principles for processing, including conditions for consent
- infringements of the data subjects' rights
- the transfers of personal data to a recipient in a third country or an international organization
- non-compliance with an order or a temporary or definitive limitation on processing or the suspension of data flows by the supervisory authority

For these categories, the maximum administrative fine will be € 20.000.000 or up to 4% of the company's worldwide turnover of the preceding financial year, whichever is higher.

If a controller or processor, either intentionally or negligently, infringes several provisions of this Regulation for the **same or linked** processing operations, the total amount of the administrative fine shall not exceed the amount specified for the gravest infringement. Fines do not keep stacking with each related infringement.

7.4 Cross-Border Data Transfer

7.4.1 'One-stop-shop'

The general rule is that the supervision of cross-border processing activity, or processing involving citizens of more than one EU country, is led by only one supervisory authority, called the 'lead supervisory authority'. This is known as the one-stop-shop principle.

The lead authority will coordinate operations involving supervisory authorities concerned, in accordance with Articles 60-62 of the Regulation (e.g. one stop shop, mutual assistance, and joint operations). It will submit any draft decision to those supervisory authorities with an interest in the matter.

Source: WP244 ANNEX II – Frequently Asked Questions

According to recital (36), in cases involving both a controller and a processor, the competent lead supervisory authority will be the authority of the member state where the controller has its main establishment. In this situation, the supervisory authority of the processor is considered a 'supervisory authority concerned' and should participate in the cooperation procedure.

7.4.2 Cross border processing

The GDPR distinguishes two types of cross-border processing:

'cross-border processing' means either:
(a) processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State; or
(b) processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State.

Source: General Data Protection Regulation (EU) 2016/679; article 4(23).

7.4.3 Multinational company

The first situation is that of a multinational company that has establishments in more than a single member state. For example, ABN-Amro is a large bank with offices in the Netherlands, Belgium, France, Germany, and other member states.

7.4.4 Internationally operating company

The second situation is that of a single establishment of a controller or processor in the union, where processing of personal data takes place which substantially affects (…) data subjects in more than one Member State. For example, this would be the type of processing that takes place at a hospital in the east of the Netherlands with patients both in the Netherlands and in Germany: The processing is 'cross border', it affects the health of individuals and an analysis of medical data, and thus special data, is carried out.

7.4.5 Substantially affect

The GDPR does not strictly define what 'substantially affect' means. Nevertheless, in December 2016 the 'article 29 working party' published guidelines[1] in which they write that supervisory authorities will interpret this on a case-by-case basis, considering:

- the context of the processing
- the type of data
- the purpose of the processing
- other factors such as whether the processing
    - causes, or is likely to cause, damage, loss or distress to individuals
    - has, or is likely to have, an actual effect in terms of limiting rights or denying an opportunity
    - affects, or is likely to affect individuals' health, well-being or peace of mind
    - affects, or is likely to affect individuals' financial or economic status or circumstances
    - leaves individuals open to discrimination or unfair treatment
    - involves the analysis of the special categories of personal or other intrusive data, particularly the personal data of children
    - causes, or is likely to cause individuals to change their behavior in a significant way
    - has unlikely, unanticipated or unwanted consequences for individuals
    - creates embarrassment or other negative outcomes, including reputational damage or
    - involves the processing of a wide range of personal data

[1] 16/EN/WP 244 http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp244_en_40857.pdf. Last viewed on 25 July 2019.

For example, a rowing club has members on two sides of a country border. Processing the addresses of the members would not be considered to 'substantially affect' the members. As a consequence, this processing would not be considered 'cross border processing'.

7.5 Regulations Applying to Data Transfer Inside the EEA

7.5.1 Identifying the lead supervisory authority

(…) the supervisory authority of the main establishment or of the single establishment of the controller or processor shall be competent to act as lead supervisory authority for the cross-border processing carried out by that controller or processor in accordance with the [cooperation] procedure provided in Article 60.
Source: General Data Protection Regulation (EU) 2016/679; article 56.

For a multinational, such as a bank, the 'main establishment' is the place of the central administration of that organization. However, if another establishment takes the decisions about the purposes and means of the processing, and has the power to have such decisions implemented, then that establishment becomes the main establishment. Consequently, the lead supervisory authority would be the authority of the member state where the main establishment is identified.

In case of a single establishment of a controller or processor in the union, where processing of personal data takes place which substantially affects (…) data subjects in more than a single member state, the lead supervisory authority is the one in the country where the establishment of the controller is.

If the processing is not likely to substantially affect data subjects 'across the border', the same supervisory authority would be supervising, but then the processing would not be considered 'cross border processing', and consequently the consistency mechanism need not be activated.

7.6 Regulations Applying to Data Transfer Outside the EEA

In general, cross border data transfers to a recipient in a third country may only take place if the transfer is made to an 'adequate jurisdiction' or if the party or parties exporting the data have implemented a lawful data transfer mechanism.

7.6.1 Transfers on the basis of an adequacy decision

A transfer of personal data to a third country or an international organization may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organization in question ensures an adequate level of protection. Such a transfer shall not require any specific authorization.
Source: General Data Protection Regulation (EU) 2016/679; article 45(1).

An 'adequacy decision' is a decision adopted by the European Commission, establishing that a third country ensures an adequate level of protection of personal data by reason of its domestic law or the international commitments it has entered into. The effect of such a decision is that personal data can flow from the EU Member States and the European Economic Area member countries (Norway, Liechtenstein and Iceland) to that third country, without any further safeguards.

The European Commission has so far (July 2019) issued adequacy decisions recognizing Andorra, Argentina, Canada (commercial organizations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, USA[2] and Uruguay as providing adequate protection.

Most of these decisions were already in place when the GDPR came into force. Article 45(4) requires the Commission to monitor developments in third countries and international organizations that could affect the functioning of those decisions. If the Commission finds that a third country, a territory (etc.) or an international organization no longer ensures an adequate level of protection (…), it can repeal, amend or suspend the decision.

7.6.2 Transfers subject to appropriate safeguards

In the absence of an adequacy decision, the controller or processor should take measures to compensate for the lack of data protection in a third country by way of appropriate safeguards for the data subject.

Such appropriate safeguards may consist of making use of binding corporate rules, standard data protection clauses adopted by the Commission, standard data protection clauses adopted by a supervisory authority or contractual clauses authorized by a supervisory authority.

Those safeguards should ensure compliance with data protection requirements and the rights of the data subjects appropriate to processing within the Union, including the availability of enforceable data subject rights and of effective legal remedies, including to obtain effective administrative or judicial redress and to claim compensation, in the Union or in a third country.

(…) Transfers may also be carried out by public authorities or bodies with public authorities or bodies in third countries or with international organizations with corresponding duties or functions, including on the basis of provisions to be inserted into administrative arrangements, such as a memorandum of understanding, providing for enforceable and effective rights for data subjects.

Source: General Data Protection Regulation (EU) 2016/679; recital (108).

When transferring data between public authorities, the public authorities must ensure compliance with the GDPR requirements. The other cases require either following an approved standard, or having protection clauses adopted by the supervisory authority.

7.6.3 Binding corporate rules (BCR)

A group of undertakings, or a group of enterprises engaged in a joint economic activity, should be able to make use of approved binding corporate rules for its international transfers from the Union to organizations within the same group of undertakings, or group of enterprises engaged in a joint economic activity, provided that such corporate rules include all essential principles and enforceable rights to ensure appropriate safeguards for transfers or categories of transfers of personal data.

Source: General Data Protection Regulation (EU) 2016/679; recital (110).

Essential requirements for the competent supervisory authority to approve a set of BCRs are

- that they are legally binding
- apply to and are enforced by every member of the group, including their employees
- expressly confer enforceable rights on data subjects with regard to the processing of their personal data
- and fulfil the requirements laid down in Article 47(2) of the GDPR

[2] The adequacy decision on the USA is limited to the Privacy Shield Network (see § 7.5.4).

This rather long list specifies, amongst others, that BCRs must specify at least:

- The data transfers, categories of data, type of processing and its purposes
- Type of data subjects affected and the identification of the third country or countries
- The application of the general data protection principles, and the requirements in respect of onward transfers to bodies not bound by the binding corporate rules
- The rights of data subjects with regard to processing and the means to exercise those rights
- The acceptance by the controller or processor established on the territory of a Member State of liability for any breaches of the binding corporate rules by any member concerned not established in the Union
- The cooperation mechanism with the supervisory authority to ensure compliance by any member of the group (…)

7.6.4 Transfers or disclosures not authorized by Union law

The GDPR limits the transfer of personal data to third countries, where third countries are countries outside the EEA.

> Any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognized or enforceable in any manner if based on an international agreement (…), in force between the requesting third country and the Union or a Member State, without prejudice to other grounds for transfer pursuant to this Chapter.
>
> Source: General Data Protection Regulation (EU) 2016/679; Article 45(1).

7.6.5 Regulations applying to data transfer between the EEA and the USA

As detailed earlier, the European Commission can take an **adequacy decision**, recognizing a country or a part of a country as having adequate data protection (GDPR, Chapter V). However, since USA data protection law differs considerably from what the GDPR, and the directive before that, require, there is no adequacy decision in place regarding the USA, either for the country or for a geographical part thereof.

Instead, in July 2016 the Commission implemented decision (EU) 2016/1250 on the adequacy of the protection provided by the EU-US Privacy Shield as issued by the US Department of Commerce. Currently, the adequacy decision regarding data transferred under the Privacy Shield is revoked[3]. It is imperative that at the moment of processing an adequacy decision is in place.

In a press release (IP-16-2461 of 12 July 2016) the European Commission described the principles the EU-U.S. Privacy Shield is based on as follows:

> Strong obligations on companies handling data:
>
> (…) the U.S. Department of Commerce will conduct regular updates and reviews of participating companies, to ensure that companies follow the rules they submitted themselves to. If companies do not comply in practice, they face sanctions and removal from the list. The tightening of conditions for the onward transfers of data to third parties will guarantee the same level of protection when of a transfer from a Privacy Shield company.

[3] You can find the full press release regarding the Privacy Shield on http://bit.ly/PDPF_privacy_shield.

Clear safeguards and transparency obligations on U.S. government access:

The U.S. has given the EU assurance that the access of public authorities for law enforcement and national security is subject to clear limitations, safeguards and oversight mechanisms. Everyone in the EU will, also for the first time, benefit from redress mechanisms in this area. The U.S. has ruled out indiscriminate mass surveillance on personal data transferred to the US under the EU-U.S. Privacy Shield arrangement. The Office of the Director of National Intelligence further clarified that bulk collection of data could only be used under specific preconditions and needs to be as targeted and focused as possible. It details the safeguards in place for the use of data under such exceptional circumstances. The U.S. Secretary of State has established a redress possibility in the area of national intelligence for Europeans through an Ombudsperson mechanism within the Department of State.

Effective protection of individual rights:

Any citizen who considers that their data has been misused under the Privacy Shield scheme will benefit from several accessible and affordable dispute resolution mechanisms. Ideally, the complaint will be resolved by the company itself; or free of charge Alternative Dispute resolution (ADR) solutions will be offered. Individuals can also go to their national Data Protection Authorities, who will work with the Federal Trade Commission to ensure that complaints by EU citizens are investigated and resolved. If a case is not resolved by any of the other means, as a last resort there will be an arbitration mechanism. Redress possibility in the area of national security for EU citizens' will be handled by an Ombudsperson independent from the US intelligence services.

Annual joint review mechanism:

The mechanism will monitor the functioning of the Privacy Shield, including the commitments and assurance as regards access to data for law enforcement and national security purposes. The European Commission and the U.S. Department of Commerce will conduct the review and associate national intelligence experts from the U.S. and European Data Protection Authorities. The Commission will draw on all other sources of information available and will issue a public report to the European Parliament and the Council.

8 Quality Aspects

8.1 Data Protection by Design and by Default

The controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organizational measures, such as pseudonymization, which are designed to implement data-protection principles, such as data minimization, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects

Source: General Data Protection Regulation (EU) 2016/679; Article 25(1).

With this article, the GDPR makes the principle of data protection **by design** a **legal requirement**, rather than just an effective way to fulfil obligations regarding data security. The controller is responsible for the implementation of a complete end-to-end set of **appropriate** technical and organizational measures.

Moreover, the GDPR states in article 25(1) that the set of appropriate technical and organizational measures is needed to integrate the necessary safeguards into the processing to (…) protect the rights of data subjects. This way a legal relationship is defined between data security principles and privacy, as the rights and freedoms of individuals.

The second paragraph of article 25 requires the controller to implement appropriate technical and organizational measures to ensure that, **by default**, only personal data are processed which are necessary for each specific purpose of the processing. This applies to the amount of personal data collected, the extent of their processing, the period of time of their storage and their accessibility.

8.1.1 The seven principles of data protection by design

The idea of data protection by design was developed by Ann Cavoukian, PhD, former Information - and Privacy Commissioner of Ontario, Canada. In a publication on the principles she wrote:

Privacy by Design is a concept I developed back in the 90's, to address the ever-growing and systemic effects of Information and Communication Technologies, and of large-scale networked data systems. Privacy by Design advances the view that the future of privacy cannot be assured solely by compliance with regulatory frameworks; rather, privacy assurance must ideally become an organization's default mode of operation.

Source: Ann Cavoukian (2011). Privacy by Design, the 7 foundational principles

The GDPR rather uses 'Data Protection by Design' (and by default), as we will do in the next paragraphs.

8.1.1.1 Proactive not Reactive; Preventative not Remedial

The Data Protection by Design approach is characterized by proactive rather than reactive measures. It anticipates and prevents privacy invasive events before they happen. Data Protection by Design does not wait for privacy risks to materialize, nor does it offer remedies for resolving privacy infractions once they have occurred; it aims to **prevent** them from occurring instead. In short, Data Protection by Design comes before-the-fact, not after.

8.1.1.2 Data Protection as the Default Setting

We can all be certain of one thing: the default rules. Data Protection by Design seeks to deliver the maximum degree of privacy by ensuring that personal data are automatically protected in any given IT system or business practice. If an individual does nothing, their privacy remains intact. No action is required on the part of a data subject to protect their privacy. Privacy and data protection are built into the system, by default.

8.1.1.3 Privacy Embedded into Design

Data Protection by Design is embedded into the design and architecture of IT systems and business practices. It is not bolted on as an add-on, after the fact. The result is that privacy becomes an essential component of the core functionality being delivered. Data Protection is integral to the system, without diminishing functionality.

8.1.1.4 Full Functionality — Positive-Sum, not Zero-Sum

Data Protection by Design seeks to accommodate all legitimate interests and objectives in a positive-sum 'win-win' manner, not through a dated, zero-sum approach, where unnecessary trade-offs are made. Data Protection by Design avoids the pretense of false dichotomies, such as privacy versus security, demonstrating that it is possible to have both.

8.1.1.5 End-to-End Security — Full Lifecycle Protection

Data Protection by Design, having been embedded into the system prior to the first element of information being collected, extends securely throughout the entire lifecycle of the data involved. That means strong security measures are essential to privacy, from start to finish. This ensures that all data are securely retained, and then securely destroyed at the end of the process, in a timely fashion. Thus, Data Protection by Design ensures cradle-to-grave, secure lifecycle management of information, end-to-end.

8.1.1.6 Visibility and Transparency — Keep it Open

Data Protection by Design seeks to assure all stakeholders that whatever the business practice or technology involved, it is in fact, operating according to the stated promises and objectives, subject to independent verification. Its component parts and operations remain visible and transparent, to users and providers alike. Remember: trust, but verify.

8.1.1.7 Respect for User Privacy — Keep it User-Centric

Above all, Data Protection by Design requires architects and operators to keep the interests of the individual uppermost, by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options. Keep it user-centric.

8.1.2 Benefits of the application of the principles of Privacy by design and privacy by default

On their website, the UK Information Commissioner's Office[4] writes:

Taking a Data Protection by Design approach is an essential tool in minimizing privacy risks and building trust. Designing projects, processes, products or systems with privacy in mind at the outset can lead to benefits which include:

- Potential problems are identified at an early stage, when addressing them will often be simpler and less costly
- Increased awareness of privacy and data protection across an organization
- Organizations are more likely to meet their legal obligations and less likely to breach the Data Protection Act
- Actions are less likely to be privacy intrusive and have a negative impact on individuals

8.2 Written Contracts Between the Controller and the Processor

GDPR article 25 requires the controller to implement appropriate technical and organizational measures and to make sure that these precautions remain in place during the processing, in fact implementing one of the Data Protection by Design principles: end-to-end security.

When a processor is engaged to carry out the processing or parts of the processing, the logical consequence is a written contract and that is exactly what the GDPR requires.

Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. (…).

Source: General Data Protection Regulation (EU) 2016/679; Article 28(3).

8.2.1 Clauses of a written contract

Article 28(3) continues: 'that contract (or other legal act) shall stipulate, in particular, that the processor:

(a) processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organization(...)
(b) ensures that persons authorized to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality
(c) takes all measures required pursuant to Article 32 (security of processing)
(d) respects the conditions (…) for engaging another processor
(e) (…) assists the controller by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights (…)
(f) assists the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 considering the nature of processing and the information available to the processor
(g) at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data

[4] https://ico.org.uk/, viewed on 25-04-2017

(h) makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller

8.2.1.1 Example

The following table shows an example of the contents of such a data processing agreement between controller and processor:

Table of contents	GDPR references
Scope and purpose of the agreement	Article 4(2) definitions: processing
Data covered by the agreement	Article 4(1) personal data; Article 9 / recital (10) special categories of personal data (sensitive data);
General security and safeguards on the processing of data	Article 32 security of processing
Technical and organizational measures	Article 28(3)(a) through (h)
Monitoring of information security and data protection	Article 35 data protection impact assessment
Information security breach and personal data breach	Article 33(2) notification of a personal data breach to the supervisory authority
Correction, deletion and blocking / specific obligations to assist the controller	Article 32 through 36
Agreement with other data processor (sub-data processor)	Article 28(2) and (4) sub processor
Transfer of data	Rec. (112), (113); Article 47 binding corporate rules; Article 49 derogations for specific situations; Chapter V transfers (..) to third countries or international organizations.
Further obligations of the processor	Article 39 tasks of the data protection officer; (1)(b) ... awareness-raising and training of staff involved in processing operations
The controller's rights of control	Article 4 (7) controller Article 28 (3)(f) assists the controller …
Return and deletion of the personal data	Article 28 (3)(g) delete or return
Duty of confidentiality	Article 28 (3)(b) confidentiality
Duration	Article 28 (3) '...contract...duration of the processing.' Article 5 principles relating to processing of personal data (1)(e) storage limitation.
Precedence	When of conflicting clauses, the GDPR takes precedence.
Signatures	

8.3 Data Protection Impact Assessment (DPIA)

The first principle of Data Protection by Design requires the controller, and in fact anyone processing personal data) to 'anticipate and prevent privacy invasive events before they happen'.

The GDPR includes this principle in Article 35:

> Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.
>
> Source: General Data Protection Regulation (EU) 2016/679; Article 35(1).

The GDPR does not require a DPIA to be carried out for every processing operation. In the 'Guidelines on Data Protection Impact Assessment and determining whether processing is 'likely to result in a high risk' (17/EN WP248) the Article 29 Working party details what a DPIA is and when conducting a DPIA is obligatory or desirable:

- A DPIA is a process designed to describe the processing, assess the necessity and proportionality of a processing and to help manage the risks to the rights and freedoms of natural persons resulting from the processing of personal data.
- A DPIA is only required when the processing is 'likely to result in a high risk to the rights and freedoms of natural persons' (Art. 35(1)).

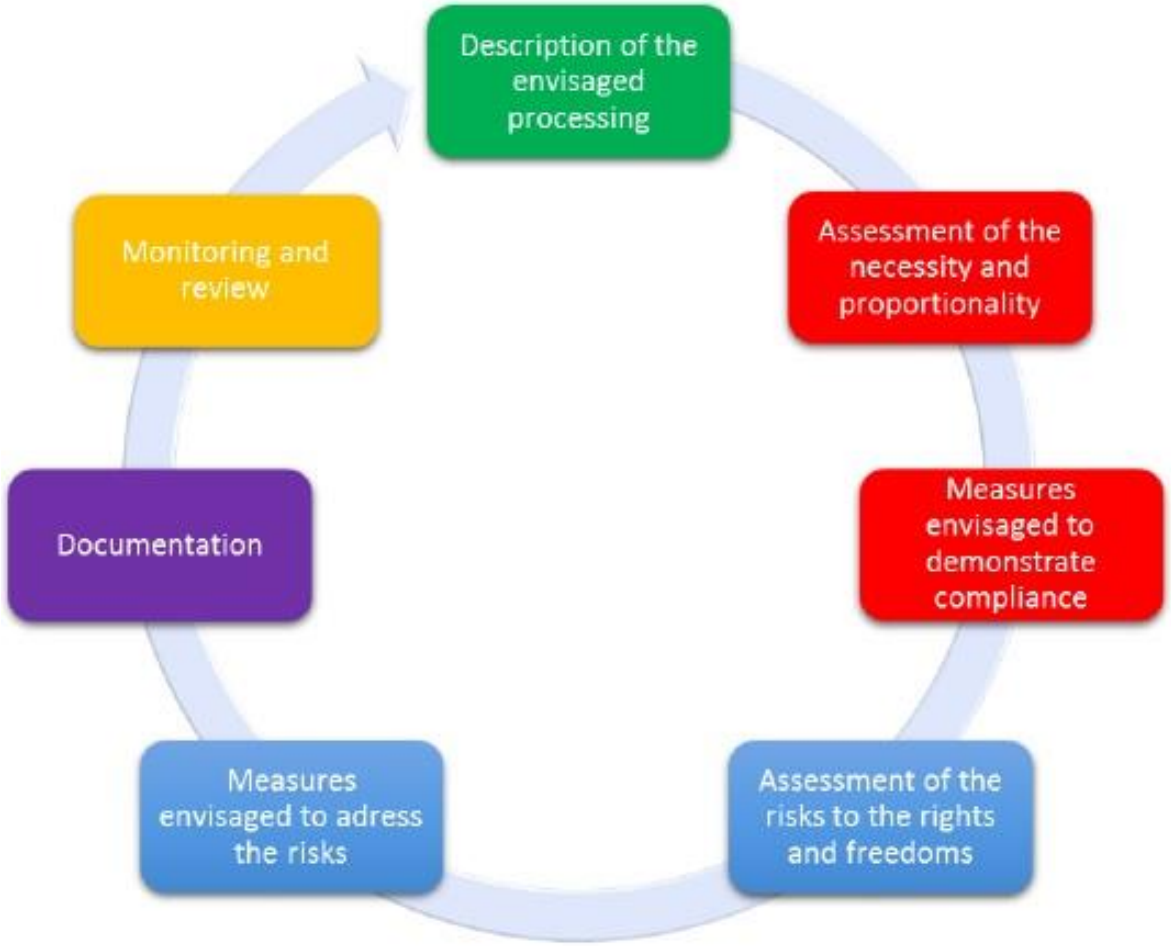
The GDPR does not define exactly what the criteria are, but provides some examples:

> (a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;
> (b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or
> (c) a systematic monitoring of a publicly accessible area on a large scale.
>
> Source: General Data Protection Regulation (EU) 2016/679; Article 35(3)

A DPIA can address a single processing operation or a set of similar processing operations. This means that **a single DPIA could be used to assess multiple processing operations that are similar in terms of the risks presented**, provided adequate consideration is given to the specific nature, scope, context and purposes of the processing. This might mean, where similar technology is used to collect the same sort of data for the same purposes.

The DPIA should be carried out **prior to the processing** (Articles 35(1) and 35(10), recitals 90 and 93). This is consistent with data protection by design and by default principles (Article 25 and recital 78).

The DPIA should be started **as early as practical** in the design of the processing operation, even if some of the processing operations are still unknown. As the DPIA is updated throughout the lifecycle project, it will ensure that data protection and privacy are considered, and promote the creation of solutions which in turn promotes compliance. It can be necessary to repeat individual steps of the assessment as the development process progresses, because the selection of certain technical or organizational measures may affect the severity of or likelihood of the risks posed by the processing.



The fact that the DPIA may need to be updated once the processing has actually started, is **not** a valid reason for postponing or not carrying out a DPIA. In some cases, the DPIA will be an ongoing process, for example where a processing operation is dynamic and subject to ongoing change. Carrying out a DPIA is a continual process, not a one-time exercise[5].

8.3.1 Objectives of a DPIA

There are a number of reasons to conduct a DPIA, such as the idea of prevention as seen in one of the Data Protection by Design principles, the obligation to document compliance, and others. In detail, a DPIA will help:

- Prevent costly changes to processes, redesign of systems or termination of projects
- Reduce the consequences of supervision and enforcement
- Improve the quality of data
- Improve service provision
- Improve decision making
- Increase privacy awareness in an organization
- Improve project feasibility
- Improve communication with regard to privacy and personal data protection
- Strengthen confidence of data subjects in the way personal data are processed and privacy is respected

[5] Picture derived from Guidelines on Data Protection Impact Assessment (DPIA), WP29 document 17/EN/248.

8.3.2 Topics of a DPIA report

The GDPR sets out the minimum features of a DPIA (Article 35(7), and recitals 84 and 90):

- a description of the envisaged processing operations and the purposes of the processing
- an assessment of the necessity and proportionality of the processing
- an assessment of the risks to the rights and freedoms of data subjects
- the measures envisaged to:
    - address the risks
    - demonstrate compliance with this Regulation

8.4 Data Lifecycle Management (DLM)

Whether data are generated by and within the organization or collected by the organization through a third party (customer, vendor, partner), the only way to effectively protect it is by understanding it. Does it contain personal data of any kind, such as customer information, employee information, sensitive communications, personally identifiable information, health information or financial data? In probably each of these cases the GDPR applies, requiring appropriate protection from the moment data are collected. Requiring a structure of privacy and security into the foundations of any project. But in fact, data changes throughout its lifetime and is often stored for years – whether for record or 'just when'. With the GDPR, however, the latter is becoming an expensive habit.

8.4.1 Purpose of Data Lifecycle Management (DLM)

Data Lifecycle Management (DLM) is a process that helps organizations manage the flow of data throughout its lifecycle: from creation, to use, to sharing, to archive and deletion.

Tracking data accurately throughout the information lifecycle is the foundation of a sensitive data protection strategy and helps determine where to apply security controls.

8.4.2 Understanding the data streams

The various requirements of the GDPR demand that a company knows:

- exactly where its data, and in particular its personal data reside
- for which purpose the data were collected or created
- for which reasons the data must be retained
- at which date or in which situation the data must be deleted

8.4.2.1 Data collection

From the very start, it is important to keep in mind which personal data are necessary for the purposes of the intended processing. The GDPR requires a reason to keep personal data stored, so at any time it must be clear and easy to at least demonstrate:

- for which purpose or purposes the information was collected
- at what date data subjects have been informed of the collection and of the purpose for processing
- whether consent has been acquired for the intended processing
- whether that consent is still valid (and not withdrawn)
- what other legal ground for processing exist

In practice, every 'piece' of information needs numerous tags indicating why it exists, and for how long it will continue to exist.

8.4.2.2 Permissions structure

Any data collection, but a collection of personal data in particular, needs a permissions structure, clearly defining which employees need, because of their role in the organization, access to which personal data.

However, things change. A good program must continually assess and review who needs access to what type or types of information. Controllers and processors should work with their IT counterparts to automate controls throughout their enterprise systems. They must make it easier for employees to do the right thing versus the wrong thing. They must avoid employees having negative consequences through their actions from simple neglect to do something.

Once the permissions structure is in place it must be maintained through regular and ongoing assessments.

8.4.2.3 Build in retention and deletion rules

One of the key principles of the GDPR is data minimization: the obligation to controllers and processors to ensure that personal data are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (Article 5(1)(c). In practice this leads to continuous balance between what data to keep and why, and what data to dispose of in a safe way.

Storing personal data is a burden for any organization. It takes effort to keep the data secure, complete and up-to-date, and even more effort to answer requests from data subjects asking for information on processing of their data, and to handle claims regarding their rights. Additionally, there is always the threat of a personal data breach, with the resulting procedures, the risk to data subjects and the risk to the company of damages, through loss of reputation, cost of remedies and possible fines.

There are many legal obligations with respect to retaining personal data for a given time. For example, think of customer registrations such as sales and financial transactions, guarantees or human resource information, such as résumés, payment history, or tax information.

Good data life cycle management

- provides the tools to manage the flow of data in an information system,
- keeps track of data from the moment it is collected or generated until the moment it is deleted because there is no **valid** reason left to retain it

8.5 Data Protection Audit

A number of articles in the GDPR mention audits as one of the methods to monitor compliance with the GDPR. For instance, in the tasks of a data protection officer (DPO):

> The data protection officer shall have at least the following tasks: to monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;
>
> Source: General Data Protection Regulation (EU) 2016/679; Article 39(1)(b).

Beside Article 39, Article 47(2)(j) requires that binding corporate rules (BCRs) shall, amongst others, specify audits to assess the mechanisms engaged to ensure verification of compliance with those BCRs.

Article 58(1)(b) gives supervisory authorities the right to carry out investigations in the form of data protection audits.

8.5.1 Purpose of an audit

The purpose of a data protection audit process is to regularly test, assess and evaluate the effectiveness of technical and organizational measures, for ensuring compliance to the GDPR, including the security of the processing.

Usually, an audit will uncover **gaps** in the privacy policies, that need to be addressed to enhance data privacy governance.

At the very least, an audit will make personal data protection the topic of the week, raising awareness throughout an organization.

Generally speaking, two types of privacy audits can be distinguished: an adequacy audit and a compliance audit.

8.5.1.1 Adequacy audit

An adequacy audit is aimed at:

- ensuring that the organization's data protection policies are applied to all instances of processing of personal data actually happening
    - including easily forgotten sets of historic data, back-ups, obsolete equipment, and so on
- assessing whether these policies are adequate to address the requirements of the GDPR and other possibly applicable data protection laws and regulations
    - both within and outside the EEA

This requires a complete understanding and mapping of data flows across the enterprise, and it is more than just reviewing all company policies, procedures, codes of practice and guidelines that affect the handling of personal data during its lifecycle. The adequacy audit should be done both within the company and with all involved third parties, such as processors.

8.5.1.2 Compliance Audit

After the adequacy audit has been completed, the next step might be, and maybe even should be, a compliance audit, in order to determine whether the organization is actually abiding by the policies and procedures identified during, and perhaps improved as a result of, the adequacy audit.

A compliance audit requires an investigation of how personal data are handled **in practice** within the various business units, across departments, and when dealing with third parties.

A comprehensive compliance audit should also examine such factors as:

- does the organization offer data privacy compliance training?
- how are data privacy policies made known to employees?
- how are complaints of policy violations handled?

The depth of the compliance audit will depend upon the perceived risks of legal violations and personal data breaches to the enterprise.

8.5.2 Contents of an audit plan

- Audit program development (planning)
  - Contacts, purposes, time frame, …
- Determining the audit approach and scope
  - Will it be an adequacy – or a compliance audit
  - Vertical (functional) audit, targeting a specific department (like 'Human Resources'), or
  - Horizontal (process) audit; tracking a particular process from one end to the other
  - Scope of the audit (data protection governance, records management, access management and data security, data protection training and awareness, etc.)
- Preparations, gathering evidence of the areas included
  - Letter of engagement
  - Contracts, like controller-processor contract, BCRs, non-disclosure agreements, etc.
  - Process descriptions; work orders, notices, …
  - Training material, flyers etc.
- Performing the audit
- Reporting
  - Overall conclusion
  - Areas of good practice
  - Areas for improvement
- Follow up

8.6 Practice-Related Applications of the Use of Data, Marketing and Social Media

8.6.1 The use of social media information in marketing activities

Not that long ago there were three methods to have the public notice the product or services a vendor was trying to sell them:

- to buy expensive advertising
- to beg mainstream media to tell their story
- to hire a huge sales force to bug people directly about the product

None of these methods were really very effective. All three methods were based on interrupting people in what they are doing, hoping that they might see the product and think: that is what I have been looking for, and if so, that they then would remember who advertised and where to find that product.

Using internet, there are better options to get your product noticed. From producers and consumers people became 'prosumers[6]', doing both product design through critiquing and consuming by spending money. It has become easy to build a website, to write a blog, to publish content and media (pictures, sound, video) on social media. Not only vendors, but virtually everyone can publish their own content, that their consumers want to buy.

Through social media, everybody can reach out to other people connected to those social media, reaching a global audience. With Facebook alone having over 1.5 billion users, a vast global market is laying wide open.

With these changes sounding in the digital age, business is becoming 'multi-channel' and interactive. Vendors write about their products like journalists, and people react to that indicating

[6] for more information, see: https://en.wikipedia.org/wiki/Prosumer

they like what they see, they like what is being produced, or they like what is on offer. Of course, if they do not like it, they will not hesitate to tell the world about that too, often in rather blunt terms.

Finally, a new sales concept is emerging. Many people find it important what other people, and in specific their friends, think of a product they are looking for. The message that '76% of your friends like this product' proves to be an incentive to buy. Even if there is no way to check this claim, we all seem to believe it.

Consumers can be divided in groups with similar taste, similar interests, and other relevant groups. When perusing a web shop, we have all seen remarks like "buyers of <the product you just looked at> also bought: <these other products>". Messages like this prove to be a very strong sales enabler, as long as the targeted consumer in fact has similar tastes and interests to those 'other buyers'.

8.6.2 Use of internet in the field of marketing

For this new and more digital economy to work, companies need information about potential buyers. In practice this means they need information about as many possible consumers as possible. What kind of consumer is it? The 'camping rough' type, needing good quality outdoor gear and clothes? The 'I want the newest technology' type? Or maybe the 'best price / performance ratio' type or rather the 'guaranteed lowest price' kind of buyer?

Profiling like that asks for a lot of data about persons and their behavior. How do these companies get that information?

8.6.3 Cookies

A cookie is just a (usually small) text file, stored at the user's computer. The most common cookies are:

- session cookies
- persistent cookies
- tracking cookies

8.6.3.1 Session cookies

Session cookies allow users to be recognized within a website, so any page changes or item or data selection the user does, is remembered from page to page. The most common example is the shopping cart feature of any web shop. Whenever items are selected, the selection is stored in the session cookie, so it is remembered until the user is ready to check out.

When logging on to a website, a session cookie in the memory of the user's computer retains the information that login was successful, as the website has no other way of remembering you logged on. When leaving the website, which usually means when closing the browser, the session cookie is erased from the memory of the user's computer, and as a result the user is logged off.

8.6.3.2 Persistent cookies

Persistent cookies remain on the user's hard drive until erased by the user or until they expire. Persistent cookies may offer simple services to the user as repeat visitor. For instance, to retain the user's language selection. When a user revisits the site it will, based on the information in the cookie, offer the content in the language chosen during the previous visit.

This type of cookie can make the website visitor's experience more personal. For example, a user uses a booking site to books a cheap flight to the British Lake district. In order for the transactions (both financial and with the airline) to succeed, the user must fill in personal information (name, address, passport number, credit card details). The next time the user visits the website, the combination of this information can lead to a more personal salutation like 'Good morning <firstname>', but also to offers of other trips, travel insurance, offers for good hiking equipment,

travel bags, and more. All based on the information gathered from the booked trip and, if applicable, earlier booked trips.

There is no need to save much information in the cookie itself. In fact, a unique identifier is enough to recognize the user (or at least his or her device or browser) and link that identifier to a database.

8.6.3.3 Tracking cookies

A tracking cookie is often called a **third-party cookie**. It is placed on a user's hard disk by a website from a domain other than the one a user is visiting.

As with regular cookies, third-party cookies placed on the user's computer make it possible to save some information about the user for use at a later time. However, third-party cookies are often set by advertising networks that a site may subscribe to.

The purpose of the cookie is to follow what pages a person is visiting, building a profile of the person based on interests. The profile can be added to, using information of other websites in their network. It is not linked to personal details known to the site, but only serves to match ads to the user's profile so that they are as relevant as possible.

8.6.4 Other profiling info: the price of 'free' services

Facebook and Google know almost everything there is to be known about the users of their free products.

> We collect the content and other information you provide when you use our services, including when you sign up for an account, create or share, and message or communicate with others. This can include information in or about the content you provide, such as the location of a photo or the date a file was created. We also collect information about how you use our services, such as the types of content you view or engage with or the frequency and duration of your activities.'
>
> Source: Facebook privacy policy

The same goes for Google. With their search engine used by billions of people, combined with information from LinkedIn, Google maps, and blog posts, Google knows what people are actively researching or buying and which words or phrases they use to find them. They know for each of their users what they are likely to buy soon, what they will need to buy now, later today, tomorrow, and more.

Google knows, because of the information they have on where we are, who we are, where we will be and what we will be doing. They know who we are, how much money we spend, what we do for a living, our demographic data (age, gender, religion, income, education), where we live, who our friends are, what we do outside of work, who we vote for, what television, podcasts, music or other entertainment we consume, and more.

Google also knows how all of these things have changed over time. This allows them to find trends and predict behavior at both an individual and an aggregate level. In short, they have exactly the information companies need to maximize their marketing. This is also the information needed to bring you the product or service you need, just at the time you need it.

8.6.5 The data protection perspective

The proposed Regulation on Privacy and Electronic Communications[7], published in January 2017 and aimed to repeal the current Directive (2002/58/EC), details the rules regarding the protection of personal data in electronic communications.

The proposed changes will bring the e-Privacy Directive in line with the GDPR. According to Article 27 of the proposal, the original intention was for the Regulation to enter into force on 25 May 2018, in parallel with the GDPR. Discussions within the Council of the European Union on details of the legal text, however, still take place almost every month. As a result, a definitive implementation of the regulation is not expected before 2020.

The Regulation on Privacy and Electronic Communications in particular targets the processing of data about the communication and the processing of metadata. Article 8 deals with 'the protection of information stored in and related to end-user's terminal equipment', i.e. with cookies, but also with spyware, hidden identifiers, web bugs and 'device fingerprinting', etc.

8.6.5.1 Cookies

> The use of processing and storage capabilities of terminal equipment and the collection of information from end-users' terminal equipment, including about its software and hardware, other than by the end-user concerned shall be prohibited, except on the following grounds: (…)
>
> Source: (draft) Regulation on Privacy and Electronic Communications (2017/0003) art. 8(1). (as viewed 6-5-2017).

The exceptions are:

(a) it is necessary for the sole purpose of carrying out the transmission of an electronic communication over an electronic communications network or,
(b) the end-user has given his or her consent or,
(c) it is necessary for providing an information society service requested by the end-user or,
(d) if it is necessary for web audience measuring, provided that such measurement is carried out by the provider of the information society service requested by the end-user

Session cookies will usually fit in either (a), (c) or (d) and as such can be stored without consent, such as in the online shopping cart discussed before.

For other cookies, consent is needed as defined in the GDPR. This consent must be freely given, specific, informed, active and unambiguous. New in the proposal is that end-users can express consent (or the lack of it) by configuring their browser settings. This will help minimize the overload of banners and pop-ups.

8.6.5.2 Profiling

There is no doubt that the GDPR applies to profiling as described, as stated explicitly in recital (72). Accordingly, the data subject has the right to object to the processing:

> Where personal data are processed for the purposes of direct marketing, the data subject should have the right to object to such processing, including profiling to the extent that it is related to such direct marketing, whether with regard to initial or further processing, at any time and free of charge. That right should be explicitly brought to the attention of the data subject and presented clearly and separately from any other information.
>
> Source: General Data Protection Regulation (EU) 2016/679; recital (70).

[7] Proposal for regulation of the European Parliament and of the council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)

A new consequence of the GDPR, in particular the right to inspection and correction, will empower the data subject a bit more than before:

> A data subject should have the right of access to personal data which have been collected concerning him or her, and to exercise that right easily and at reasonable intervals, in order to be aware of, and verify, the lawfulness of the processing.
>
> This includes the right for data subjects to have access to data concerning their health, for example the data in their medical records containing information such as diagnoses, examination results, assessments by treating physicians and any treatment or interventions provided.
>
> Every data subject should therefore have the right to know and obtain communication in particular with regard to the purposes for which the personal data are processed, where possible the period for which the personal data are processed, the recipients of the personal data, the logic involved in any automatic personal data processing and, at least when based on profiling, the consequences of such processing.
>
> Where possible, the controller should be able to provide remote access to a secure system which would provide the data subject with direct access to his or her personal data. That right should not adversely affect the rights or freedoms of others, including trade secrets or intellectual property and in particular the copyright protecting the software. However, the result of those considerations should not be a refusal to provide all information to the data subject.
>
> Where the controller processes a large quantity of information concerning the data subject, the controller should be able to request that, before the information is delivered, the data subject specify the information or processing activities to which the request relates.
>
> Source: General Data Protection Regulation (EU) 2016/679; recital (63)

But there are still a lot of 'free' services around, offering content or other free products or services, provided the user consents to their gathering information about them, their interests and taste in order to 'select appropriate advertising'. The GDPR will not change this completely, but it will at least give us the chance to correct this information.

It is up to the data subject to be careful with the information revealed to companies offering newsletters or other free services. As cited above, as soon as a data subject becomes aware of a company tracking their behavior, objecting to this processing should be successful.

The point is that most people are used to consenting to lengthy statements without actually reading them. The GDPR forbids the lengthy, unreadable statement and requires simple, clear language explaining what the personal data collected is to be used for.

8.7 Big Data

The current processing of massive amounts of information from customers (or rather, from everybody who uses the internet) in order to build the profiles described in the previous paragraphs, illustrate the remark in the first paragraph of this document.

The challenge was, and still is, to find a balance between concerns for the protection of personal freedoms and the possibility to support free trade throughout Europe.

There is reason for doubt whether 'privacy' really has a future at all. Although the GDPR clearly indicates that the European Commission takes its obligation, as stated in recitals (1) and (2), seriously:

> The principles of, and rules on the protection of natural persons with regard to the processing of their personal data should, whatever their nationality or residence, respect their fundamental rights and freedoms, in particular their right to the protection of personal data. This Regulation is intended to contribute to the accomplishment of an area of freedom, security and justice and of an economic union, to economic and social progress, to the strengthening and the convergence of the economies within the internal market, and to the well-being of natural persons.
>
> Source: General Data Protection Regulation (EU) 2016/679; recital (2)

Contact EXIN

www.exin.com