# Introduction to the General Data Protection Regulation

## 1. Introduction

The General Data Protection Regulation (GDPR) is one of the most ambitious legal projects of the European Union in the last years. From 25 May 2018 the GDPR will replace the Data Protection Directive and the data protection laws in 28 Member States will become obsolete to a large extent. Only those companies that start adapting their contracts, business processes and IT solutions pursuant to the GDPR in a timely manner will achieve a prudent level of compliance when the GDPR applies from 25 May 2018.

Not only the high fines of up to EUR 20 million or 4% of the total worldwide annual turnover illustrate that companies must take the GDPR seriously. Data protection has become one of the largest compliance risk areas and therefore necessarily a priority for the management of every company.

The below introduction allows the reader to quickly get an overview of the GDPR or certain parts of the GDPR. For certain details, the introduction refers to specific articles of the GDPR or specific comments of articles of the GDPR in the commentary section of this book.

## 2. The most important compliance steps to be implemented before the GDPR applies from 25 May 2018

The GDPR will apply from **25 May 2018** (Art. 99 para. 2). To achieve minimum compliance with the GDPR by then, controllers and processors must begin with compliance steps sooner rather than later.

For controllers the most important compliance steps to be implemented by 25 May 2018 can be summarised as follows:

1) implementation of a basic **data protection compliance programme** (see chapter 11 below) including the appointment of a **data protection officer**, to the extent reasonable or required in the particular case (see chapter 14 below);
2) preparation of a **record of processing activities** (see chapter 12 below);
3) review of the legal basis of the respective data processing operation (see chapter 7 below), in particular the new requirements regarding valid consent (see chapter 7.2 below);
4) development of GDPR compliant **privacy notices** (see chapter 8 below); and
5) review of the legal basis for **international data transfers** (see chapter 18 below).

For processors the most important compliance steps to be implemented by 25 May 2018 can be summarised as follows:

1) appointment of a **data protection officer** to the extent required or reasonable in the particular case (see chapter 14 below);
2) preparation of **records of processing activities** (see chapter 12 below);
3) implementation of **appropriate security measures** (see chapter 15.1);
4) ensuring that **subprocessors** are engaged only with prior specific or general written authorisation of the controller (Art. 28 para. 2); and
5) assurance that **international data transfers** take place only if compliant with the requirements of the GDPR (see chapter 18 below).

The above-mentioned measures will not produce full compliance with the GDPR but they help to focus the personnel and financial resources of a controller or processor on central compliance aspects.

For larger organisations it will also be required to assess generally in advance the regulatory risks resulting from the GDPR to allow for an efficient deployment of resources.

## 3. Basic terms of the GDPR

The GDPR exclusively applies to **personal data** (see chapter 4.1 below). Personal data are defined as any information relating to an identified or identifiable **natural** person, who is referred to as the **data subject** (Art. 4 No. 1).

A subset of personal data is **sensitive data** (also 'special categories of personal data'). Sensitive data are defined in Art. 9 para. 1 as personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, data concerning a natural person's sex life or sexual orientation, data concerning health within the meaning of Art. 4 No. 15, genetic data within the meaning of Art. 4 No. 13 and biometric data (eg, fingerprints or facial images) if processed for the purpose of uniquely identifying a natural person (Art. 9 cmt. 3). Furthermore, social security numbers might be regarded as sensitive data (cf. Art. 4 cmt. 35).

The GPDR applies to controllers and processors (cf. Art. 3 cmt. 4). The GDPR defines the term **controller** as the natural or legal person which, alone or jointly with others, determines the purposes and means of the processing of personal data (Art. 4 No. 7).

**Processor** means a natural or legal person which processes personal data on behalf of the controller, that is, that it does not determine the purposes and means of the processing of personal data (Art. 4 No. 8). For example, if a company outsources the operation of its customer database to an IT service provider, the company still acts as a controller, whereas the IT service provider acts as a processor.

**Processing** is defined broadly as any operation which is performed on personal data such as the collection, recording, structuring, alteration, retrieval, use, disclosure by transmission, erasure or destruction (Art. 4 No. 2).

The term **transfer** is used quite frequently throughout the GDPR. However, it is not defined. Transfer includes the disclosure vis-à-vis another controller or processor, respectively a subprocessor (see Art. 44 cmt. 1).

The term **supervisory authority** means the data protection authority respectively established by each Member State.

## 4. The scope of the GDPR

The following provides an outline concerning: (i) the processing activities that are covered by the GDPR (see chapter 4.1 below), (ii) those to whom the GDPR applies (see chapter 4.2 below), and (iii) where the GDPR applies (see chapter 4.3 below).

### 4.1 Material scope – what processing activities are covered?

The GDPR generally applies to any processing of personal data. As set out above under chapter 3, personal data means any information relating to an **identified or identifiable natural person**. Whether a natural person is identifiable must be assessed **objectively**, not only taking into consideration the legal and factual possibilities of the controller, but also the possibilities of third parties (Art. 4 cmt. 3). For example, the IP address of a user constitutes personal data for the operator of a website, even if the operator of the website cannot identify the person but only the Internet access provider can identify the user (see decision of the CJEU, C-582/14 – Breye/Germany regarding the interpretation under the Data Protection Directive; see also the statement of the advocate general).

If data relate to **legal persons**, they only constitute personal data pursuant to the GDPR if the name of the legal person contains the name of a natural person (Art. 4 cmt. 1). Moreover, data that relate to deceased persons do not constitute personal data within the meaning of the GDPR (Art. 4 cmt. 2).

The GDPR basically only applies to **data processed by automatic means**. For data that is processed manually (generally on paper) the GDPR applies only if the personal data form part of a filing system or if they are intended to form part of a filing system (Art. 2 para. 1). 'Filing system' means any structured set of personal data which are accessible according to specific criteria (Art. 4 No. 6) such as HR files organised pursuant to names. Individual paper-based files are not subject to the GDPR (Art. 2 cmt. 4).

As an act of law of the Union, the GDPR does not apply to matters which fall outside the scope of Union law (eg, national security; see Art. 2 para. 2 lit. a). Furthermore, the GDPR does not apply to common foreign and security policy (Art. 2 para. 2 lit. d) or to the areas of the prevention, investigation, detection or prosecution of criminal offences and the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security (Art. 2 para. 2 lit. d; in these areas, Directive (EU) 2016/680 applies which will have to be implemented separately into national laws).

Furthermore, the GDPR does not apply to the processing of personal data by natural persons in the course of a purely personal or household activity ('**household exemption**'; Art. 2 para. 2 lit. c). This covers in particular the use of social networks for private purposes (Art. 2 cmt. 7).

### 4.2 Personal scope – who does the GDPR apply to?

The GDPR applies to controllers and processors (see chapter 3 above regarding the definition of these terms).

Under the Data Protection Directive the role of the processor was advantageous because the processor was subject to only a few regulatory obligations. The commercial disadvantage was – and still is – the obligation to not use personal data for one's own purposes and to not commercially exploit them. If a company wants to use personal data for its own purposes and wants to commercially exploit the data (ie, is aiming for '**data ownership**'), the company has to be qualified as a controller which results in substantial additional obligations.

This has been changed by the GDPR because the GDPR applies to processors as it does to controllers and therefore makes processors subject to substantial regulatory obligations (see chapter 2 above) and subject to the same administrative fines (see chapter 20 below). Due to the alignment of obligations of controllers and processors, the commercial advantages of being a controller will become more attractive. Many companies that have so far limited themselves to being a processor, will likely try to move into a controller role. This would not only result in the applicability of regulatory obligations regarding the legal basis of the data processing such as consent of the data subject (see chapter 7 below) and transparency requirements (see chapter 8 below), but also in the requirement to revise existing contracts with customers, vendors and data subjects to reflect the new regulatory reality.

### 4.3 Territorial scope – where does the GDPR apply?

The GDPR applies to controllers and processors that are **established in the EU or the EEA** (see Art. 3 cmt. 5). Processors in the EU are subject to the GDPR even if they process data for controllers that are not subject to the GDPR (Art. 3 cmt. 4).

Furthermore, the GDPR applies if the controller, respectively the processor, is not established in the EU or the EEA, but has an establishment (eg, an affiliate) in the EU or in the EEA and the processing of personal data takes place **in the context of the activities of this establishment**. This applies, for example, if the US parent company processes personal data of customers of a German or Austrian affiliate to support the sales activities of that affiliate (see Art. 3 cmt. 2).

To ensure that companies that do not have an establishment in the EU/EEA but are active in the European market are subject to the same conditions of competition as European companies, the GDPR also applies to controllers and processors that are not established in the Union if they are **offering their goods or services, irrespective of whether a payment is required, in the Union, respectively the EEA** (Art. 3 para. 2 lit. b).

Furthermore, the GDPR applies to controllers and processors that are not established in the Union, but monitor the behaviour of data subjects in the Union (Art. 3 para. 2 lit. b). This applies in particular to online advertising networks which log the web browsing activities of Internet users to deliver personal online advertisement.

## 5. The relationship with national data protection laws

Like any EU regulation, the GDPR in general applies directly and may not be implemented by national law. The previously existing national data protection laws will therefore be largely superseded by the GDPR as of 25 May 2018.

Outside the scope of the GDPR (see chapter 4 above) national legislatures may enact additional data protection provisions. For example, this applies to data protection laws regarding legal persons where it remains to be seen whether Member States will make use of this possibility. In any case, taking into account the protection under the national laws transposing the Trade Secrets Directive (2016/943/EU), a blanket regulation of personal data relating to legal persons does not seem warranted.

Notwithstanding the above, there are numerous topics within the scope of the GDPR for which the GDPR does not (or not comprehensively) provide an answer but expressly authorises Member States through **opening clauses** to enact national laws. The GDPR therefore allows for deviations among Member States. This applies in particular to the following topics (cf. Art. 92 cmt. 4):

1) How old must a minor be to validly consent to the processing of his/her personal data? (Art. 8 para. 1 subpara. 2)
2) When is it not possible to validly consent to the processing of sensitive data? (Art. 9 para. 2 lit. a)
3) Is the processing of genetic data, biometric data or health data subject to additional limitations? (Art. 9 para. 5)
4) Is it permitted at all to process personal data on criminal convictions and offences? (eg, in connection with a whistleblower hotline; Art. 10)
5) Are automated individual decisions and profiling that are not necessary for the performance of the contract with the data subject permitted without consent of the data subject? (Art. 22 para. 2 lit. b)
6) Are the rights of data subjects subject to additional limitations? (Art. 23)
7) Do all controllers and processors have to appoint a data protection officer or only certain controllers and processors? (Art. 37 para. 4)
8) Is it possible to impose administrative fines on public authorities and bodies? (Art. 83 para. 7)
9) May data protection NGOs claim damages on behalf of data subjects? (Art. 80 para. 1)
10) May data protection NGOs initiate legal proceedings against a controller or a processor without a data subject's mandate? (Art. 80 para. 2)

Additionally, the GDPR grants the Member States a very far-reaching legislative competence for the processing of employees' personal data in the **employment context** (Art. 88) and allows the Member States to regulate the processing of personal data for journalistic purposes and the purposes of academic, artistic or literary expression (Art. 85) and to find reconciliation between the right to public access to official documents and the right to the protection of personal data (Art. 86).

As a result, the GDPR must always be read together with the respectively applicable national 'GDPR implementation act'. Therefore, the GDPR is also called a '**limping regulation**'. It is problematic that the GDPR does not contain any '**conflict of law**' provisions. Therefore, it remains unclear when to apply the law of which Member State.

In our opinion, this is an unintended gap which must be solved by analogy to the rules of competence under the GDPR (see chapter 19 above). If there is a lead

competence of a certain supervisory authority for a controller or processor pursuant to Art. 56, the 'GDPR implementation act' of such Member State applies (see in detail Art. 92 cmt. 5).

### 6. The principles relating to the processing of personal data

The GDPR stipulates the following principles that must be complied with whenever personal data is processed (Art. 5 para. 1):

1) **Lawfulness** (Art. 5 para. 1 lit. a): Personal data must be processed lawfully, that is, a legal basis for the processing is required (see chapter 7 below).
2) Fairness (Art. 5 para. 1 lit. a): Personal data must be processed fairly which is of relevance in particular when conducting a balancing of interests test (see, eg, Art. 6 para. 1 lit. f).
3) **Transparency** (Art. 5 para. 1 lit. a): Personal data must be processed in a transparent manner in relation to the data subject. This principle is further specified by the information obligations contained in the GDPR (see chapter 8 below).
4) **Purpose limitation** (Art. 5 para. 1 lit. b): The first element of the purpose limitation principle is that personal data may only be collected if an explicit and legitimate purpose was specified no later than at the time of the collection (principle of **purpose specification**). This may, for example, be done by documenting the processing purposes in the record of processing activities (see chapter 12 below). Since the processing purposes must be legitimate, other laws (eg, consumer protection law) must indirectly also be taken into consideration in data protection assessments. The second element of the purpose limitation principle requires that collected data may not be further processed in a manner that is incompatible with the purposes originally specified (**purpose limitation in a strict sense**) unless the data subject consented (Art. 6 cmt. 12). Whether the purposes are compatible must be assessed by applying certain criteria stipulated in Art. 6 para. 4. If the new purpose is compatible with the former (original) purpose, the processing is permitted without the need for a new legal basis (eg, new consent) (cf. Art. 6 cmt. 14). However, data subjects must be informed about the new processing purpose (Art. 13 para. 3 and Art. 14 para. 4).
5) **Data minimisation** (Art. 5 para. 1 lit. c): The type and scope of the processed data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed. This principle is a specification of the general principle of proportionality. It would be regarded excessive and therefore a violation of the data minimisation principle if, for example, in order to document the used data volume of each employee, a company does not only log the size of the downloaded files but also the file name and the time of a download.
6) **Accuracy** (Art. 5 para. 1 lit. d): Personal data must be accurate and, where necessary for the processing purpose, kept up to date.
7) **Storage limitation** (Art. 5 para. 1 lit. e): Personal data may be stored no longer than necessary for the specified purposes for which the personal data

are processed. Upon expiration of that period, data must be deleted or anonymised. For example, due to the principle of storage limitation, the storage of documents regarding a contractual relationship to defend against potential claims of a customer would violate the GDPR after the statutory limitation period expired.

8) **Integrity and confidentiality** (Art. 5 para. 1 lit. f): Contrary to its name, this principle does not only require appropriate measures to protect the integrity and confidentiality of personal data, but also measures to protect availability and lawfulness of the processing. 'Security and lawfulness' would therefore be the more appropriate name for the principle in Art. 5 para. 1 lit. f (see Art. 5 cmt. 11).

The principles relating to processing of personal data are complemented by the principle of **accountability** which requires that the controller implements compliance measures to ensure compliance with the above-mentioned principles and that the controller is able to demonstrate compliance with these principles (Art. 5 para. 2). The second element of the accountability principle does not shift the burden of proof (which would not be compliant with the presumption of innocence), but results in a material obligation to demonstrate compliance. A violation of this material obligation is not subject to any administrative fines but only to the enforcement powers of the competent data protection authority (Art. 5 cmt. 13).

*This is an extract from the chapter 'Introduction to the General Data Protection Regulation' by Lukas Feiler, Nikolaus Forgó and Michaela Weigl in* The EU General Data Protection Regulation (GDPR): A Commentary, *published by Globe Law and Business.*