# Legal Update –

# General Data Protection Regulation (GDPR)

January 2018

A brief overview of the new EU data protection law.

In spring 2018, precisely on May 25th, a new chapter of data protection law will begin. The EU General Data Protection Regulation becomes effective and will replace the national data protection acts of all EU member states which are based on the EU Data Protection Directive 95/46 (hereinafter: "95/46/EC"). The purpose of the GDPR is to align the standards of the data protection law of every member state, ensuring the same high protection level in each. In order for this to work, the new data protection law is enacted as a regulation, meaning that the law is applicable in every member state without any further legislative acts. Companies should seek to adapt the requirements of the new law at an early stage so as to avoid the strengthened sanctions which can be imposed by the Data Protection Authorities. Within this overview, we explore some of the key changes within the GDPR and potential problem areas ahead of its implementation.

## Responsibility and sanctions

Due to the new regulation, data protection supervisory authorities ("DPAs") will soon be able to impose fines that are much more substantial in value. Infringements of the legal provisions can be subject to administrative fines up to EUR 20 million or 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher. This raise of sanctions gives an understanding of the value of data and the importance of data protection in the 21st century.

## Material and territorial scope of the GDPR

The goal of the GDPR is to protect and prevent breaches of data. The focus is upon natural persons (also referred to as "data subjects") for whom the GDPR provides protection from unwanted and unlawful processing. Importantly, data relating to legal entities is not captured within the material scope of the regulation.

The previsions of the GDPR are binding to every data controller or data processor with a headquarter or a subsidiary within the European Union, just as it is under the current law. Furthermore – and this is new – it applies also to every data controller that is not established in the Union, but whom offers goods and services within the Union or processes data of natural people which are in the territory of the Union.

## Accountability, documentation and data protection impact assessment

Pursuant to Article 5 (1) of the GDPR, it is mandatory for the data controller to comply with the principles relating to the processing of personal data. As already known from the 95/46/EC these principles are, among others, the lawfulness, fairness and transparency of the processing of data. Beyond that, the GDPR demands in Article 5 (2) that the data controller is able to demonstrate its compliance with these principles at every time ("accountability"). If he cannot demonstrate compliance, he may face sanctions from the DPA.

Furthermore, every data processor is obliged by the GDPR to maintain a record of its processing activities. In this regard, it is worth noting that this record of processing activities also enables the data controller to fulfil a bulk of its accountability obligations, regulated in Article 5 (2) and Article 24. The obligation to maintain a processing record applies to every data controller that processes data not just occasionally but rather systematically. In assessing this requirement, systematic use of data should be considered unavoidable if a company processes data for either regular customer contact or the internal administration of the employees. As opposed to the 95/46/EC the GDPR foresees this obligation also for every data processor.

Where a certain type of data processing is likely to result in a higher risk to rights and freedom of the natural person whose data is processed, the data controller is also obliged to carry out an assessment of the possible impact of the envisaged processing operations (a "data protection impact assessment"). Such higher risk exists for example when using new processing technologies to conduct an extensive evaluation of personal aspects of the natural person on automated processing and profiling or because of processing a large scale of special categories of data like health data. Where a data protection impact assessment is required, the result of this exercise must be documented and reviewed as appropriate.

## Data transfer and responsibility

The data transfer between companies based in EU member states has to be compliant with the GDPR. Due to the fact the obligations of the GDPR are the same in every member state one can say that the transfer of data within the EU becomes easier.

The transfer of data to recipients based outside the EU, like in the USA, requests further measures. For example, a company that is planning to transfer data to another company in the States has to ensure that its contractual partner is certified under the Privacy Shield. Alternatively, the contracting parties have the possibility to use the EU standard data protection clauses to assure that the recipient is compliant to the rules of the GDPR.

The establishment of binding corporate rules ("BCR") within a corporate group becomes more easy to implement under the GDPR. Because of the "consistency mechanism", stated in the GDPR, such internal guidelines are valid and accepted in every member state, once a DPA of one single member state has approved and certified these rules.

The processing of data by a third party, normally an external company ("processor") – e.g. in the field of cloud computing – will be highly regulated under the GDPR. Contrasted to the legal provisions on the processing of data by a third party in the 95/46/EC, the new regulation introduces a number of requirements to the processing of data by the processor. Though it was already mandatory under the current law to conclude a data processing agreement, if data was meant to be processed by a third party, the new law stipulates more requirements for this contract. Out of this change emerges the need to adapt the already existing processing agreements to new legal requirements. One of the bigger changes is that the data processor will be liable directly to the data subject in case of a data breach where this arose within the scope of its responsibility.

Likewise, the legal construct of the joint controllership is a new feature of GDPR. This gives companies the possibility to share the responsibility of data processing between two different controllers. Although the joint controllership doesn't allow a transfer of data between parties, it provides the possibility of exploring new business models; involving more than one company as a controller, allowing them to easily share the responsibility for the processed data.

## Data subject rights and information obligations

Of particular importance under the GDPR are the rights of the data subject. Although notification of certain data breaches to the DPA was mandatory before, the GDPR again sets tighter requirements to this procedure.

A key development of the GDPR is the extension of the existing right to *erasure* so to afford data subjects a new right to be forgotten. This obligates the controller not just to erase the data of the data subject if asked to do so, but to also undertake reasonable steps to make sure that any other copy of the specific data that may have been published by the controller will be erased. This obligation requires greater effort on the part of the data controller than before.

Another new data subject right is the right to data portability. This right grants the possibility to reclaim the personal data that the data subject has previously provided to the data controller. The data controller has to provide the requested data in a structure commonly used and machine-readable format. The purpose of this provision is to enable the data subject to transmit this data to another controller, e.g. when changing the provider of a certain system like an app-service.

Further bolstering the rights of the data subject are the newly arising obligations upon the data controller. These obligations may require the data controller to consider whether it has effective processes to so as to enable it to respond to data subject requests and the exercise of the above data subject rights. If the controller does not fulfil

these requirements, an impacted data subject has the option to file a complaint with the DPA. As mentioned before, the DPA is authorised to impose significant fines. Furthermore, the data subject can claim damages from the data controller for not fulfilling its obligations under the GDPR with no undue delay and in any event within one month from the receipt of the request.

Moreover, the data controller is obliged to fulfil information duties to a larger extent than before. These changes will have a significant impact in particular with regard to data privacy policies for websites. For example, from May 2018 onwards the following must be declared:

- The contact details of the data controller as well as those of the data protection officer ("DPO") where applicable;
- the legal basis of the processing (by naming the specific justification within the GDPR that allows the processing); and,
- the period for which the personal data will be stored, or at least the criteria used to determine that period.

In this field, the E-Privacy-Regulation, which takes effect in May 2018 as well, will regulate the important obligations concerning the operation of websites and the data protection in the online sector in generally

## Processing data in the context of employment

Every employer has to consider the rules of the GDPR concerning the data of its employees – for example with regard to GPS-Tracking or CCTV – especially data subject rights and the information obligations.

As an initial step, works agreements with employees should be reviewed against the provisions of the GDPR. Such agreements have to comply with the transparency requirement in Article 88 (2) of the GDPR and must reveal to the employee what kind of data is about to be processed.

## Notification in case of data breach

The codified obligation to notify in case of a data breach will become more important as well. At present there is an obligation to notify only in case of a breach or violation of special categories of personal data, e.g. health data of a natural person. In those circumstances the controller has the obligation to notify the DPA immediately. This obligation becomes tighter under the GDPR and will be triggered by a breach or violation of the requirements in respect of any kind of personal data. It makes no difference whether the breach is caused by an unlawful access to the data or by an accidental instance of erasure. The controller has to notify the DPA without undue delay and not later than 72 hours after having become aware of it if the data breach may result in a risk to the rights and freedoms of a data subject. The obligation to notify does not occur however there is no risk for any personal data.

This obligation necessitates a data management system that enables the controller not only to monitor the data processing but also forecast the severity of any breach so as to determine whether there is a need to notify the DPA within the required time limits. You will appreciate that an inaccurate prediction of the risk to personal data in either direction can be problematic; meaning that it is within the interests of the data controller to get this right.

## To Do's

What do you have to do now? It is obvious that the GDPR has its roots in the 95/46/EC. Hence the legal requirements of the GDPR are not completely new and unknown. Nevertheless, the changes in data protection law are immense and require a lot of adjustments in the daily routine of every company. That's why every person responsible for a company should have in mind the 25 May 2018 and ensure their compliance with the requirements of the GDPR on time. Based upon our experience and know-how operating in this sector we recommend the following steps to implement and monitor GDPR-compliance:

- Analyse any data processing within the company
- Upon completion of the above, compare the company's data processing activities with the requirements of the GDPR (GAP-Analysis and risk assessment)
- Use the GAP Analysis/Risk Assessment process to inform the required implementation of the legal provisions of the GDPR
- Ongoing monitoring of the data processing

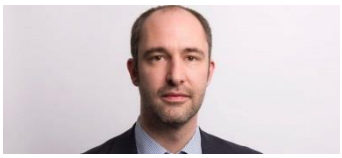
## How we can help you

The lawyers at DWF look back on years of experience advising on data protection law. Based on this experience we are able to assist your business' transition to full legal compliance with the requirements of the GDPR. Furthermore, our lawyers also possess a detailed understanding of the underlying technologies and are well versed in communicating with both IT departments and technology partners to bridge the gap between the legal requirements and corresponding possible technical solutions.


**Klaus Brisch, LL.M. (USA)**
Partner
Leiter Technologiesektor DWF weltweit
Fachanwalt für Informationstechnologierecht
**T** +49 221 534098-0
**E** klaus.brisch@dwf.law

**Marco Müller-ter Jung, LL.M. (Informationsrecht)**
Partner
Fachanwalt für Informationstechnologierecht
**T** +49 221 534098-0
**E** marco.mueller-terjung@dwf.law

**Thorsten Jansen, LL.M. (Sydney)**
Senior Associate
**T** +49 221 534098-0
**E** thorsten.jansen@dwf.law



**Florian Daniel, LL.M. (Medienrecht)**
Senior Associate
**T** +49 30 25090110-0
**E** florian.daniel@dwf.law

**Claudia Rehse**
Senior Associate
**T** +49 221 534098-0
**E** claudia.rehse@dwf.law

**Nathalie Eichler**
Associate
**T** +49 30 25090110-12
**E** natalie.eichler@dwf.law

**Daniel Groß**
Associate
**T** +49 221 534098-0
**E** daniel.gross@dwf.law

**Nico Czajkowski, LL.M.**
Associate
**T** +49 221 534098-0
**E** nico.czajkowski@dwf.law