The European General Data Protection Regulation

Constantin Herfurth, Trainee lawyer in Munich
Philian Hole, B.A., in Kassel

March 2017

[1] The European General Data Protection Regulation (GDPR) will largely replace the German Federal Data Protection Act (BDSG) after a two-year transition period. From 25 May 2018, the Regulation will apply uniformly and directly in all Member States throughout the EU. Companies in Germany must therefore review their current data protection management on the basis of the new legal situation and adapt it if necessary. This review is part of the company's own risk management, because any breaches of the General Data Protection Regulation can result in considerable disadvantages for companies. The possible fines on the part of the supervisory authorities have been drastically increased to up to 20 million EUR or, in the case of a company, up to 4 % of the total annual turnover achieved worldwide in the previous business year (Art. 83 para. 5 GDPR). In addition, there is the threat of claims for damages by data subjects (Art. 82 GDPR) and legal action by associations (Art. 80 GDPR). If any breaches become known to the public, there is also the threat of considerable damage to the company's reputation. The goal of every company must therefore be to analyse and subsequently minimise these risks.

Starting point: Processing of personal data

The starting point of data protection law is the personal data. Only when such data is processed, the General Data Protection Regulation is applicable at all (Art. 2 para. 1 GDPR). According to Art. 4 no. 1 GDPR, this is understood to be any information relating to an identified or identifiable natural person. A person is identifiable if he or she 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 one or more special characteristics. If, on the other hand, anonymous data are processed, the provisions of data protection law do not apply (Recital 26 GDPR). "Data processing" means any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, filing, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction (Art. 4 no. 2 GDPR).

To understand whether the provisions of the General Data Protection Regulation apply to them, companies

[1] Constantin Herfurth is a research assistant at the Scientific Centre for Information Technology Design (ITeG) at the University of Kassel. Philian Hole is a Bachelor of Arts B.A. Law-Economics-Personnel and a staff member at the Department of Public Law, IT Law and Environmental Law at the University of Kassel.

should get an overview of their data flows and check whether they process personal data.

Responsibility

If personal data are processed, the General Data Protection Regulation provides for various regulations and obligations to act to protect the data subjects. In order to implement these regulations effectively, it must be clear who is to take the resulting measures. First of all, therefore, it must be clarified: "Who is responsible for what towards whom?". According to Art. 4 no. 7 GDPR, the controller is 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. It is not a question of who formally decides on the data processing, but who actually initiates and significantly influences it. The actor identified thereafter ("who?") is responsible for the processing of personal data in accordance with the General Data Protection Regulation ("for what?") vis-à-vis the data subject and further supervisory authorities ("vis-à-vis whom?").

General data processing principles

If a company is responsible for processing personal data in accordance with the General Data Protection Regulation, it seems useful to first get an overview of the system and the main objectives of the Regulation. The general principles for the processing of personal data in Art. 5 GDPR can provide assistance in this regard:

- Lawfulness (Art. 5 para. 1 lit. a GDPR)
- Transparency (Art. 5 para. 1 lit. a GDPR)
- Purpose limitation (Art. 5 para. 1 lit. b GDPR)
- Data minimisation (Art. 5 para. 1 lit. c GDPR)
- Accuracy (Art. 5 para. 1 lit. d GDPR)
- Storage limitation (Art. 5 para. 1 lit. e GDPR)
- Data security or "integrity and confidentiality" (Art. 5 para. 1 lit. f GDPR)
- Accountability (Art. 5 para. 2 GDPR)

These principles are taken up again in many places in the Regulation and concretised by detailed regulations. They are therefore briefly described below.

Lawfulness

According to Art. 5 para. 1 lit. a GDPR, any processing of personal data must have a legal basis. Without a legal basis, data processing is prohibited (so-called prohibition principle). Such a legal basis can arise either from the General Data Protection Regulation or from other Union law or Member State law. In the General Data Protection Regulation, Art. 6 GDPR is the central provision on the lawfulness of data processing. According to this provision, processing is lawful if at least one of the following conditions is met:

- Consent of the data subject (Art. 6 para. 1 lit. a GDPR)
- Necessity for the performance or conclusion of a contract (Art. 6 para. 1 lit. b GDPR)
- Necessity for the fulfilment of legal obligations (Art. 6 para. 1 lit. c GDPR)
- Necessity for the protection of vital interests (Art. 6 para. 1 lit. d GDPR)
- Necessity for the performance of public tasks (Art. 6 para. 1 lit. e GDPR)
- Necessity for the protection of legitimate interests (Art. 6 para. 1 lit. f GDPR)

After companies have obtained an overview of their data flows, they should in a next step check on which legal bases their data processing is currently based and whether these can continue beyond 25 May 2018. This applies in particular to legal bases from national law.

Transparency

According to Art. 5 para. 1 lit. a GDPR, data processing must be transparent to the data subject. The data subject should understand that personal data concerning him or her are being collected, used, accessed or otherwise processed and to what extent the personal data are currently being processed and will be processed in the future (Recital 39 GDPR). For this purpose, the GDPR provides for information obligations of

the controller (Art. 13 and 14 GDPR) and a right of access of the data subject (Art. 15 GDPR). All this information must be provided by the controller in an easily understandable manner, without delay and free of charge (Art. 12 GDPR).
Companies should first determine whether they have any processes in place to fulfil their transparency obligations. If so, they should compare to what extent and in what form they currently provide information and whether this complies with the new requirements of Art. 12 et seqq. GDPR.

Purpose limitation

According to Art. 5 para. 1 lit. b GDPR, the controller must determine specific legitimate purposes for which the data are to be processed. These purposes must be determined before the initial data collection. If they are not determined until later or not at all, there is unlawful data processing "in stock". If the personal data are processed further in the future, the controller is still bound by the original purposes. Processing for other purposes (so-called change of purpose) is only possible under strict conditions (Art. 6 para. 4 GDPR).
Companies should therefore make sure that a purpose is defined before the personal data is collected and that this is documented (for example in a processing directory in accordance with Art. 30 GDPR). If the data is to be processed later for a different purpose, it must be checked beforehand whether a change of purpose is permissible.

Data minimisation

According to Art. 5 para. 1 lit. c GDPR, data may only be processed to the extent necessary to achieve the purpose. First, the controller must check whether personal data are necessary at all to achieve the purpose or whether anonymised data can be processed instead (Rectial 39 GDPR). If the first is the case, then the personal data must be limited to what is necessary. The guideline for this is: "As little data as possible, as much data as necessary".
Companies should check to what extent their existing data processing complies with this principle and make adjustments if necessary.

Accuracy

According to Art. 5 para. 1 lit. d GDPR, the processing of personal data is only permissible if the data is complete, correct and (where necessary) up-to-date. This makes it necessary for the controller to regularly check the accuracy of the data on its own initiative. If the data is found to be inaccurate, it must be corrected or deleted. The same applies in the event that a data subject asserts a justified right to rectification (Article 16 GDPR) or deletion (Article 17 GDPR).
Companies must therefore ensure that they have structures in place that allow for a regular review of the data. For the reaction to rectification and deletion claims, they should implement appropriate workflow processes (as with transparency obligations).

Storage limitation

According to Art. 5 para. 1 lit. e GDPR, personal data may only be stored for as long as is necessary to achieve the purpose. Afterwards, the data must be deleted (Art. 17 para. 1 lit. a GDPR). An exception to this applies if the company has legal obligations to retain data, for example under the German Commercial Code (HGB) (Art. 17 para. 3 lit. b GDPR).
Companies must check which deletion periods apply to them and then establish an individual deletion concept that complies with the requirements of Art. 17 GDPR.

Data security

According to Art. 5 para. 1 lit. f GDPR, the controller must ensure secure processing of the data ("integrity and confidentiality"). Data security in this context means in particular protection against destruction, loss, alteration or unauthorised disclosure of personal data (Art. 32 para. 2 GDPR). The required level of protection depends on the risk assessment. The higher the risk is to be assessed, the stronger the protective measures the controller must take.
It is imperative that companies check whether the existing processing standards meet these requirements. If weaknesses are discovered, appropriate measures to improve data security must be implemented.

Accountability

Article 5 para. 2 GDPR imposes on the controller the obligation to document and, if necessary, prove the lawful processing of data in accordance with the aforementioned principles. In the event of a dispute, the controller must be able to prove that the processing was carried out in accordance with the requirements of the General Data Protection Regulation.
For companies, this means that it is imperative to fully document their data processing in order to be able to prove the lawfulness of their actions in case of conflicts.

Outlook

The General Data Protection Regulation, which will come into force in 2018, will entail a not inconsiderable amount of additional work for companies. Depending on the current state of data protection management, the complexity of the data processing operations and the available resources in the company, the two-year transition period until the deadline may be tight. Many companies have therefore already started with the implementation. All others should check as early as possible where they stand now, and which steps still need to be taken by 25 May 2018.

+ + +

The Alliuris Group

The Alliuris Group consists of 20 law firms and 400 business lawyers within Europe, Asia and America.

Contact	Alisha Daley-Stehr Alliuris Communication
Web	www.alliuris.law
Mail	info@alliuris.org
Fon	+49-511-307 56-20
Fax	+49-511-307 56-21

Alliuris in Germany

Firm	Herfurth & Partner Luisentraße 5, D-30159 Hanover
Web	www.herfurth.de
Fon	+49-511-307 56-0
Fax	+49-511-307 56-10
Mob	
Contact	Ulrich Herfurth, Partner
Languages	German, English, French, Spanish, Portuguese, Russian, Mandarin, Czech, Polish
Mail	info@herfurth.de

IMPRINT

EDITORS: ALLIURIS A.S.B.L. ALLIANCE OF INTERNATIONAL BUSINESS LAWYERS | BRUSSELS

MANAGEMENT: Luisenstr. 5, D-30159 Hannover
Fon +49-511-307 56-20, Fax +49-511-307 56-21

BRUSSELS · PARIS · LONDON · AMERSFOORT · UTRECHT · KNOKKE · LUXEMBURG · LYON · MADRID · BARCELONA · LISBON · MILAN · COPENHAGEN · HANOVER · ZUG · VIENNA · SALZBURG · MOSCOW MINSK · ATHENS · ISTANBUL · BEIJING · SHANGHAI · GUANGZHOU NEW DELHI · MUMBAY · NEW YORK · MEXICO CITY SAO PAULO · RIO DE JANEIRO · BRASILIA · BUENOS AIRES · LIMA

EDITORIAL DEPARTMENT
Ulrich Herfurth, Rechtsanwalt