Paul Voigt · Axel von dem Bussche

The EU General Data Protection Regulation (GDPR)

A Practical Guide

Springer

The EU General Data Protection Regulation (GDPR)

Paul Voigt • Axel von dem Bussche

The EU General Data Protection Regulation (GDPR)

A Practical Guide

Springer

Paul Voigt
Taylor Wessing
Berlin, Germany

Axel von dem Bussche
Taylor Wessing
Hamburg, Germany

ISBN 978-3-319-57958-0 ISBN 978-3-319-57959-7 (eBook)
DOI 10.1007/978-3-319-57959-7

Library of Congress Control Number: 2017942999

Printed on acid-free paper

This Springer imprint is published by Springer Nature
The registered company is Springer International Publishing AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Contents

Introduction and 'Checklist'

1

Data protection standards are becoming increasingly high, and companies face the more and more complex task to evaluate whether their data processing activities are legally compliant, especially in an international context. Data—by their very nature—can easily cross borders and play a key role in global digital economy. Over the last couple of years, data have become a valuable asset and are even called the currency of the future.[1] The processing of personal data takes place in various spheres of economic and social activity, and the progress in information technology makes the processing and exchange of such data considerably easier.[2] In this context, the European Union (EU) adopted the General Data Protection Regulation (GDPR) to further harmonise the rules for data protection within the EU Member States and to raise the level of privacy for the affected individuals. The GDPR will enter into force on 25 May 2018. Due to its wide, transnational scope of application, it will also affect numerous companies located outside the EU. Entities should evaluate whether they fall within the scope of application of the GDPR and try to reach compliance with its requirements in a timely manner.

1.1 Legislative Purpose and Previous Legal Provisions

1.1.1 The Data Protection Directive

More than 20 years ago, the European Community (now the *EU*) felt a need to align data protection standards within their Member States in order to facilitate EU-internal, cross-border data transfers. At that time, national data protection laws provided considerably different levels of protection and could not offer legal

[1]Reiners, ZD 2015, 51, 55; Martini, in: Paal/Pauly, DSGVO, Art. 25 (2017), rec. 45—calling data the 'commodity of the 21st century'.

[2]Rec. 4 Data Protection Directive 95/46/EC.

P. Voigt, A. von dem Bussche, *The EU General Data Protection Regulation (GDPR)*,
DOI 10.1007/978-3-319-57959-7_1

certainty—neither for individuals nor for data controllers and processors.[3] In 1995, the European Community therefore adopted *Directive 95/46/EC* of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (in short: the *Data Protection Directive*) in order to harmonise the protection of fundamental rights of individuals with regard to data processing activities and to ensure the free flow of personal data between EU Member States.[4]

European directives are not directly applicable in all EU Member States but have to be transposed into national law. Thus, they require implementation measures in each EU Member State. The Data Protection Directive did not live up to its objectives and failed to align the level of data protection within the EU. Legal differences arose as a consequence of the implementing acts adopted by the various EU Member States. Data processing activities that were allowed in one EU Member State could be unlawful in another one with regard to the specific execution of data processing.

1.1.2 The General Data Protection Regulation

In 2016, the *GDPR* has been adopted to replace the Data Protection Directive from 1995. It is the result of a tough negotiation process entailing numerous amendments to the legal text that took 4 years until the adoption of the finalised Regulation.

The fragmentation of data protection across EU Member States and the resulting legal uncertainties were considered to constitute an obstacle to the pursuit of economic activities at EU level and lead to a distortion of competition.[5] In contrast to the Data Protection Directive, the Regulation *directly applies* to its addressees—no further implementation measures by the EU Member States required. By equalising the rules for data protection, the GDPR shall lead to more legal certainty and remove potential obstacles to the free flow of personal data.

The EU aims at regaining the people's trust in the responsible treatment of their personal data in order to boost digital economy across the EU-internal market.[6] For this purpose, companies will be facing new data protection obligations, as well as a reinforcement of pre-existing obligations under the GDPR. The legislator took into account the challenges of a global economy, new technologies and new business models and therefore created a very wide scope of application that will affect numerous companies. As not only data protection duties but also the impending fines have been significantly increased, companies should carefully reorganise their internal data protection procedures in order to reach compliance with the GDPR.

[3] Polenz, in: Kilian/Heussen, Computerrechts-Handbuch, Grundbegriffe (2013), rec. 3.

[4] Rec. 3 GDPR.

[5] Rec. 9 GDPR.

[6] Recs. 7, 9 GDPR.

1.2 Checklist: Most Important Data Protection Obligations

In order to give a *cursory overview* of the data protection requirements under the GDPR, the following 'checklist' *summarises* the *essential obligations* imposed on data processing entities, along with references to the respective chapters and sub-chapters of this handbook.

1.2.1 Organisational Requirements

Entities will have to make considerable efforts to get their data protection organisation into compliance with the GDPR. Different organisational requirements will have to be fulfilled.

Records of Processing Activities
Controllers and processors will have to implement records of their processing activities that will—if thoroughly maintained—permit to prove compliance with the GDPR towards the Supervisory Authorities and help to fulfil the information obligations towards the data subjects. Records must contain, inter alia, information on the purposes of processing, the categories of data that are affected and a description of the technical and organisational security measures applied. Section 3.4 provides for details on content and purpose of the records, as well as the—in practice rarely applicable—exceptions from this obligation.

Designation of a Data Protection Officer
Private entities are obliged to designate a Data Protection Officer if their core activities, meaning activities that are decisive for their business strategy, consist of regular and systematic monitoring of data subjects or of processing special categories of personal data (such as health data) on a large scale. Groups of undertakings are free to designate a single Data Protection Officer for all or several of the group entities. Any Data Protection Officer must be designated based on its expertise and professional qualities in order to ensure that it can successfully carry out its responsibilities, such as monitoring the entity's compliance with the GDPR. Details are available in Sect. 3.6.

Data Protection Impact Assessment
If an intended processing activity, in particular using new technologies, is likely to result in a high risk to the rights and freedoms of the data subjects, entities must carry out a preventive Data Protection Impact Assessment to identify appropriate measures for mitigating the risks to data protection. If the results of the assessment do not enable the entity to determine which safeguards could be applied, it will have to consult with the Supervisory Authorities. The latter might issue black- and whitelists in the future that clarify what processing activities will require a Data Protection Impact Assessment. For details on the scope of and affected processing activities by the assessment, see Sect. 3.5.

Data Protection by Design and by Default
The GDPR puts emphasis on preventive data protection concepts. As the obligation to develop and implement such concepts is directly enforceable, entities should address the concepts of Privacy by Design and Privacy by Default; see Sect. 3.7. This concerns especially entities whose processing activities consist of processing of vast amounts of personal data; see Sect. 9.1.

Technical and Organisational Measures
Entities must implement technical and organisational measures to guarantee the safeguard of personal data. The appropriate data protection level must be determined based on the risk potential inherent to the entity's processing activities on a case-by-case basis. Details on how to determine the risk potential and the appropriate security measures are available in Sect. 3.3.

Data Subject Rights
Individuals will have comprehensive information and other rights against data processing entities. The latter will have to proactively fulfil numerous obligations towards the data subjects, such as granting information on processing, erasing personal data or rectifying incomplete personal data. Especially, the data subjects' right to data portability may challenge entities as they will have to provide datasets to their customers upon request. Details on the different data subject rights are available in Chap. 5.

Data Breach Notification
The GDPR introduces a general reporting duty of the controller towards the Supervisory Authorities in case of a personal data breach. Such breach might occur by way of a technical or physical incident. The notification has to take place within a 72-hour time frame after becoming aware of the breach. In case of an incident with a high risk for the rights and freedoms of the data subjects concerned, the controller will have to communicate the breach also to them. In such a case, assistance from the Supervisory Authority will be available to the controller. Further details are available in Sect. 3.8.

Data Protection Management System
Where feasible based on an entity's budget and resources, compliance with the GDPR might be implemented and monitored by way of a Data Protection Management System. It is an internal compliance system that will monitor the fulfilment of the data-protection-related and safety-related requirements. See Sect. 3.2.1 for details, and for a four-step approach regarding its practical implementation, see Chap. 10.

Appointment of a Representative by Non-EU Entities
Entities that fall within the scope of application of the GDPR without having an establishment in the EU are obliged to appoint an EU-located representative. The

latter shall serve as contact point for data subjects and the Supervisory Authorities. For details, see Sect. 4.3.8.

Codes of Conduct and Certifications
While not mandatory, a self-regulation mechanism, such as Codes of Conduct and Certifications, will have greater practical relevance under the GDPR. Whereas Codes of Conduct specify the obligations under the GDPR for a certain sector or technology, Certifications will prove compliance of the certified activities with the GDPR. The use of these instruments will facilitate the burden of proof for compliance towards the Supervisory Authorities. For details, see Sect. 3.9. Moreover, entities may use these instruments as safeguards for third country data transfers. For details, see Sect. 4.3.6.

1.2.2 Lawfulness of the Processing Activities

Apart from their obligation to implement the different organisational requirements under the GDPR, entities must ensure the lawfulness of processing, including as regards intra-group processing activities, data transfers to third countries and the involvement of a processor.

Legal Bases for Processing
Any processing activity is forbidden unless it is justified by law. Most of the available legal bases for processing under the GDPR were already provided for in the Data Protection Directive. The requirements for obtaining valid consent have been tightened up, as described in Sect. 4.2.1. Other legal permissions for processing include its contractual necessity or prevailing legitimate interests of the controller. Moreover, a change of the data processing purpose is only permissible in limited cases. For details, see Sect. 4.2.2.5.

Intra-Group Processing Activities
The GDPR does not provide for an intra-group privilege, and each group entity will be accountable for its own data protection standards. Thus, intra-group data transfers must be justified by law generally to the same extent as data transfers to third parties. For details, see Sect. 4.4.

Special Categories of Personal Data
Special categories of personal data relate, inter alia, to an individual's political opinions, religious or philosophical beliefs or health. They merit specific protection, and processing of such data must be subject to appropriate safeguards based on its high risk potential. As HR data usually contain information on an employee's health, entities will be affected by these restrictions in practice. In this regard, they must bear in mind that processing of special categories of personal data is forbidden unless covered by, inter alia, the data subject's consent or its necessity in an employment or social security context. Details on the different kinds of special

categories of personal data, as well as the legal conditions for processing them, are available in Sect. 4.2.3.

Involvement of a Processor
Under the GDPR, the processor does not qualify as a third party. Thus, its involvement lies in the sole discretion of the controller and does not require a legal ground. It should be noted that the same goes for processors located in third countries. Nevertheless, the controller must make sure to choose a suitable processor that can guarantee for an appropriate level of data protection. In this regard, the processor is facing its own enforceable organisational obligations under the GDPR. Further details are available in Sect. 3.10.

General Requirements for Third Country Data Transfers
Where personal data shall be transferred to recipients located outside the EU, such transfer must be subject to specific safeguards in order to guarantee for an appropriate level of data protection. Entities must verify in a two-step approach (1) that this processing activity is covered by a legal justification (for details, see Sect. 4.2) and (2) that appropriate safeguards will be applied. The different safety measures are described in detail in Sect. 4.3. From a company perspective, the ones with the highest practical relevance are as follows.

EU Standard Contractual Clauses
The data exporter located inside the EU and the data importer located outside the EU can conclude a contract based on the EU Standard Contractual Clauses. These are sets of contractual clauses that are adopted by the European Commission or national Supervisory Authorities. If those clauses are used completely and unaltered, they serve as an appropriate safeguard for international data transfers. Section 4.3.3 provides for further details.

EU–U.S. Privacy Shield
Data transfers to the U.S., which often occur in corporate structures, might be based on the EU–U.S. Privacy Shield. This is a legal framework adopted by the European Commission, which allows U.S. entities to obtain a (self-)certification for an appropriate data protection level. The Privacy Shield principles as well as its mode of operation and an outlook on recent developments are available in Sect. 4.3.4.

Binding Corporate Rules
Groups of undertakings or entities involved in a joint economic activity might adopt Binding Corporate Rules that define the group members' global privacy policy with regard to the international transfers of personal data to those group members located in third countries that do not provide an adequate level of protection. Their mode of operation, minimum content and adoption procedure are explained in detail in Sect. 4.3.5.

References

Martini M (2017) Art. 25 DSGVO. In: Paal BP, Pauly DA (eds) Beck'sche Kompaktkommentare Datenschutz-Grundverordnung, 1st edn. C.H. Beck, Munich

Polenz S (2013) Rechtsquellen und Grundbegriffe des allgemeinen Datenschutzes. In: Kilian W, Heussen B (eds) Computerrechts-Handbuch, supplement 8/2013. C.H. Beck, Munich

Reiners W (2015) Datenschutz in der Personal Data Economy – Eine Chance für Europa, ZD, pp 51–55

Scope of Application of the GDPR

2

Compliance with the GDPR might require entities to carry out a time- and money-consuming reviewing process of their current data protection standards. As a result, companies might need to adjust their data processing structures and processes. Thus, in a first step, companies should find out whether they will be affected by the entering into force of the GDPR.

2.1 In Which Case Does the Regulation Apply?

Article 2 – Material Scope

1. 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.

[. . .]

To summarise its material scope, the GDPR applies to *any processing of personal data*. The Regulation will become relevant for companies as soon as any data processing takes place. The (material) scope is interpreted in a *very broad manner* in order to ensure a high level of protection.

2.1.1 'Processing'

'Processing' means any *operation* or set of operations that is *performed on personal data* or on sets of personal data, whether or not by automated means, Art. 4 No. 2 GDPR. Basically, any treatment of data will be considered as processing. Examples include collecting, recording, organising, structuring, storing and erasing of data. The open wording results from the legislators' intention to prevent any risk

P. Voigt, A. von dem Bussche, *The EU General Data Protection Regulation (GDPR)*,
DOI 10.1007/978-3-319-57959-7_2

of circumvention and to make the scope of application independent from technological change.[1] It includes processing carried out *wholly* as well as *partially by automated means*, the latter meaning any processing where certain steps are carried out by individuals, such as entering data into a computer system.[2]

Example

- personal data processing through the use of computers, smartphones, webcams, dashcams, camera drones
- collection of personal data through wearables or other smart devices (such as cars)[3]

The wide definition of 'processing' also includes a short-term use of small amounts of personal data.[4]

Example

- Personal data is intermediately being stored on an IT system, such as in the cache of a browser.
- Personal data is displayed on a computer screen.

Manual Processing

By definition, manual processing of data is considered 'processing' under the GDPR. In contrast to automatic processing through technology, manual processing is being entirely *executed by humans* without using tools or machines. By its very nature, this works much slower and less data can be processed. Therefore, manual processing only falls within the definition of 'processing' under the GDPR if *two conditions* are being met:

- Said data must be contained or be intended to be contained in a *filing system* (Art. 2 Sec. 1 GDPR). Based on predefined structure rules, a filing system divides data into different groups that are systematically managed.
- Those files must be *structured* according to *specific criteria*.[5] The Regulation does not specify any requirements for those specific criteria. Given prior legislation and the broad manner of interpretation of the GDPR, for example, chronically organised files, alphabetically organised files or files organised according to pre-determined categories should meet those conditions.[6]

[1] Rec. 15 GDPR.

[2] Ernst, in: Paal/Pauly, DSGVO, Art. 2 (2017), rec. 6.

[3] Examples drawn from Ernst, in: Paal/Pauly, DSGVO, Art. 2 (2017), recs. 5–6.

[4] Laue/Nink/Kremer, Datenschutzrecht, Einführung (2016) rec. 10, see also for the following examples.

[5] Rec.15 GDPR.

[6] Plath, in: Plath, BDSG/DSGVO, Art. 2 (2016), rec. 7.

Example

A medical practice stores its patient data in paper records. The paper records are structured alphabetically based on the patients' surnames within several filing cabinets. There is a drawer for surnames starting with 'A', one for surnames starting with 'B' and so forth.

In this example, the patient data is filed alphabetically based on different groups of letters. Thus, the records are contained in a filing system structured according to a specific criterion and the GDPR applies.

2.1.2 'Personal Data'

As shown above, any systematic handling of data corresponds to the notion of 'processing' under the material scope of the GDPR.[7] Data means (electronically) stored information, signs or indications. However, data has to be 'personal' in order to fall within said scope of application of the Regulation. Data is deemed personal if the information relates to an *identified or identifiable individual*, Art. 4 No. 1 GDPR. Data is therefore personal if the identification of a person is possible based on the available data, meaning if a person can be detected, directly or indirectly, by reference to an identifier. This is the case if the assignment to one or more *characteristics* that are the expression of a physical, physiological, psychological, genetic, economic, cultural or social identity is possible, for example:

- a person's name[8];
- identification numbers, such as a social insurance number, a personnel number or an ID number;
- location data;
- online identifiers (this may involve IP addresses or cookies[9]).

The Regulation does not apply to personal data of a *deceased person*.[10] However, at the same time, said data can be personal data of a relative or a descendant of the deceased.[11] For example, such data could give information on hereditary diseases of a descendant.[12]

[7]Barlag, in: Roßnagel, DSGVO, Anwendungsbereich (2017), rec. 7.

[8]Barlag, in: Roßnagel, DSGVO, Anwendungsbereich (2017), rec. 8.

[9]Rec. 30 GDPR.

[10]Rec. 27 GDPR.

[11]Ernst, in: Paal/Pauly, DSGVO, Art. 4 (2017), rec. 6; Schild, in: Wolff/Brink, BeckOK, Art. 4 (2016), rec. 5; see also Dammann, in: Simitis, BDSG, § 3 (2014), rec. 17.

[12]See also Dammann, in: Simitis, BDSG, § 3 (2014), rec. 17.

2.1.2.1 Identifiability of the Data Subject

As aforementioned, an individual does not need to be identified already. The mere possibility of identification, 'identifiability', will render data 'personal' under the GDPR. Identification is made possible by *combining different information* that by themselves would not have traced back to the person but does so in combination. The wording of Art. 4 No. 1 GDPR does not state who needs to be able to identify the data subject, suggesting that the additional information does not necessarily have to be in possession of the data controller/processor.

Relative Criteria

Under the former Data Protection Directive, all means 'likely reasonably' (Rec. 26 Data Protection Directive) to be used for acquiring additional information from *whatever source* had to be taken into account in order to determine identifiability. However, it has been controversially discussed whether relative or absolute criteria had to be used to establish *reasonable likeliness of identifiability*.[13] Using absolute criteria would mean that the definition of 'personal data' is being met as soon as *anyone would have the possibility* to connect the processed data to an individual.[14] In October 2016, the ECJ ruled that the risk of identification appears insignificant in reality if it requires a disproportionate effort in terms of time, cost and manpower, the aforementioned being *relative criteria*.[15] Thus, if the identification of the data subject would be possible for the controller/processor based on its chance to access additional information without disproportionate effort, the data is deemed 'personal data'. Even though the ruling is based on the Data Protection Directive, there are indications within the GDPR that such relative criteria should continue to apply.[16] Hence, a person can be considered as identifiable if the *missing information* that would allow identification is *(easily) accessible*, for instance, because it is published on the Internet or in a (commercial) information service. Also, the knowledge of third parties has to be considered as soon as there is a chance that the controller/processor receives access to such knowledge. Upon reversion, if there is no chance that the controller/processor could access the additional information, a person is not considered identifiable.

[13]For sources on both opinions, see Voigt, MMR 2009, 377, 378 et seq.; Bergt, ZD 2015, 365, 365 et seq.

[14]See also Herbst, NVwZ 2016, 902, 904.

[15]ECJ, ruling of 19 October 2016, Breyer./.Federal Republic of Germany, C-582/14, rec. 46; Opinion of the Advocate General, 12 May 2016, C-582/14, rec. 68.

[16]Such as rec. 26 GDPR using the terms 'all the means reasonably likely to be used' and 'account should be taken of [...] factors, such as the costs of and the amount of time required for identification'; approvingly, see Piltz, K&R 2016, 557, 561; Barlag, in: Roßnagel, DSGVO, Anwendungsbereich (2017), rec. 9 et seq.; Schreiber, in: Plath, BDSG/DSGVO, Art. 4 (2016), rec. 9; disapprovingly see Buchner, DuD 2016, 155, 156.

Circumstances of the Individual Case
Furthermore, in order to affirm identifiability, the circumstances of the individual case have to be taken into account. This includes the following[17]:

- the *costs and time* required for identification;
- the technology available at the time of the processing and *technological developments*;
- the purpose of the processing.

The requirement of taking into account technological developments might prove difficult in practice, as this means that data controllers/processors need to include foreseeable or likely technological developments in their decision-making processes.[18] If the purpose of the processing can only be achieved upon knowledge of the data subjects' identity, it can be assumed that the data controller/processor has the means for identification.[19] In short, the faster and easier an individual can be made out, the more likely it is an 'identifiable individual'.

2.1.2.2 Anonymisation and Pseudonymisation

Anonymisation
Anonymisation is a way of *modification* of personal data with the result that there is/remains *no connection* of data *with an individual*. Anonymised data is either information that does not relate to an identified or identifiable individual or personal data that was rendered anonymous in such a manner that the person is not or no longer identifiable.[20] Anonymisation can be achieved through a number of *techniques* that generally fall within *two categories*:

1. *Randomisation*: it consists of altering the accuracy of data in order to remove the strong link between the data and the individual. If the data becomes sufficiently uncertain, it can no longer refer to a specific individual.[21]
2. *Generalisation*: it consists of generalising/diluting the attributes of data subjects by modifying the respective scale or order of the data (i.e., a region rather than a city, a month rather than a week).[22]

In case of an effective anonymisation, the *GDPR does not apply*.[23] Anonymisation is commonly used in connection with statistical or research purposes. However, if

[17]Rec. 26 GDPR.
[18]Piltz, K&R 2016, 557, 561.
[19]See also Art. 29 Data Protection Working Party, WP 136 (2007), p. 19 et seq.
[20]Rec. 26 GDPR.
[21]See also Art. 29 Data Protection Working Party, WP 216 (2014), p. 12.
[22]See also Art. 29 Data Protection Working Party, WP 216 (2014), p. 16.
[23]Rec. 26 GDPR.

the controller/processor can restore the anonymised information with reasonable likelihood, it will be deemed personal data under the GDPR.

Example

For its upcoming 20th anniversary, a private tuition service provider wants to find out how many of its former students attended a university and, if so, what they studied. For this purpose, the service provider collects the data of its students from the past 20 graduation years and contacts them via email to participate in an online survey. In order to anonymise the data, the survey does not contain questions on the name, email address, graduation year or date of birth. The IP addresses of the participants are not being recorded. Furthermore, in order to avoid the identification of former students who graduated in more unusual study subjects, the latter are being regrouped into study areas, such as 'natural sciences', 'legal and business studies', 'social and educational studies' and 'language and cultural studies'.[24]

In this example, the tuition service tries to avoid collecting information that would allow singling out individuals, such as based on their names, dates of birth or even unusual study objects. By minimising the amount of collected data to what is absolutely necessary to carry out its survey, the likelihood of re-identification becomes extremely small. Thus, the anonymisation is successful and the GDPR does not apply.

Benefits of Anonymisation

Anonymisation offers a number of benefits for the controller/processor. Entities often store and collect very large (sometimes even excessive) amounts of data, even though they ultimately only need a small part of the data for their processing activities. The *non-collection or deletion* of the excess data can help to render data anonymous, which will prevent the applicability of the GDPR. This way, the controller/processor does not have to fulfil the multiple data protection obligations (see Chap. 3) under the GDPR. Additionally, such *data minimisation* can save time, money and staff resources. Entities should take the coming into force of the GDPR as an opportunity to consider using anonymisation as a tool to safeguard privacy.

Practical Advice[25]

As the EU does not provide for a standard of successful anonymisation, a combination of randomisation and generalisation techniques should be considered for stronger privacy guarantees.

As a *risk factor* is always inherent to anonymisation, this must be considered when assessing possible techniques corresponding to the severity and likelihood of the identified risk. As a consequence, the optimal solution needs to be determined on a case-by-case basis. This includes evaluating the *context* of the *data processing*

[24] See also Dammann, in: Simitis, BDSG, § 3 (2014), rec. 201 et seq.

[25] See Art. 29 Data Protection Working Party, WP 216 (2014), pp. 6, 7, 12, 16, 23–25.

situation: 'all' the means 'likely reasonably' available for (re-)identification need to be taken into account.

When the optimal solution has been found, its implementation requires careful engineering to enhance the robustness of the technological outcome.

Once implemented, the anonymisation technique requires *constant monitoring* in order to control the inherent risks, above all the identification potential of the non-anonymised part of the database.

Pseudonymisation

Pseudonymisation is a common tool to avoid the possibility to identify an individual through data. Pseudonymisation is defined as the processing of personal data in such a manner that the personal data can *no longer be attributed* to a specific data subject *without* the *use of additional information*, Art. 4 No. 5 GDPR. This could be achieved by replacing the name or other characteristics with certain indicators. The additional information potentially allowing identification must be kept *separately*. Also, pseudonymisation must be further ensured by additional technical and organisational measures. This could be achieved by *encoding* the information and sharing the key with only a few people.

Please note that, unlike anonymous data, pseudonymised data still falls within the scope of *application of the GDPR*, as the risk of re-identification is higher with pseudonymised data than with anonymous data. However, pseudonymisation constitutes one possibility for processors and controllers to meet their data protection obligations under the GDPR as it can facilitate to prove compliance with the Regulation[26]:

- Pseudonymisation constitutes an appropriate measure for achieving data protection through technology (see Sect. 3.7).
- Pseudonymisation might diminish the risk potential of processing in such a way that the controller will not be obliged to notify a personal data breach regarding the pseudonymised data (see Sect. 3.8).
- Pseudonymisation could constitute a sufficient safeguard to justify a change of the data processing purpose (see Sect. 4.2.2.5).
- Successful pseudonymisation might be positively taken into account whenever the controller's interests are balanced against the data subject's interests, for example, where data processing shall legally be based on prevailing legitimate interests of the controller (see Sect. 4.2.2.2).

Example

A group of undertakings consists of, inter alia, entities A and B. A is collecting personal data of the group's customers, while B receives the collected data for profiling (customer preferences and others). However, before the data is

[26]Rec. 28 GDPR; Laue/Nink/Kremer, Datenschutzrecht, Einführung (2016), rec. 27, see the latter also for the following remarks.

provided to B, it is pseudonymised by removing personal customer information, such as names and addresses, and replacing it with reference numbers. The assignment rule for these reference numbers is deposited with the group's Data Protection Officer who has been instructed not to disclose the assignment rule to employees of B.

In this example, B is unable to link the data to the respective customer without the assignment rule and the latter is unknown to B. Thus, the personal data is pseudonymised for B. However, the data is not anonymous and the GDPR is still applicable because there is still a certain risk of re-identification. It cannot be excluded with reasonable likeliness that B will not figure out the rule or the identity of certain customers, for example, through other employees (e.g., of entity A) or in case the Group Data Protection Officer infringes its instructions.[27]

Successful pseudonymisation can guarantee data privacy. Upon reversion, if the applied pseudonymisation technique cannot sufficiently safeguard the additional information, the data protection obligations under the GDPR have to be fulfilled by way of other or additional technical and organisational measures.[28]

2.1.3 Exemptions from the Scope of Application

Article 2 Sec. 2 GDPR provides for four exceptions as to the material scope of application. Among others, the Regulation does not apply in the areas of security policy (lit. b) or criminal persecution (lit. d). The most important exception from an economic point of view is provided for in lit. c, according to which the 'Regulation does not apply to the processing of personal data by an individual in the course of a *purely personal or household activity*'. This notion should be interpreted based on the general social opinion and includes personal data that is being processed for leisure activities, hobbies, vacation or entertainment purposes, for the use of a social network or data that is part of a personal collection of addresses, birthdays or other important dates, such as anniversaries.[29]

It should be noted that if processing concerns both private and business information, the exception will not be applicable.[30] The word 'purely' implies such *narrow interpretation* of this exception.[31] A business activity should include any economic

[27]Example drawn from Laue/Nink/Kremer, Datenschutzrecht, Einführung (2016), rec. 30.

[28]Rec. 26 GDPR.

[29]Ernst, in: Paal/Pauly, DSGVO, Art. 2 (2017), rec. 18; rec. 18 GDPR; Plath, in: Plath, BDSG/DSGVO, Art. 2 (2016), rec. 13.

[30]Rec. 18 GDPR; Plath, in: Plath, BDSG/DSGVO, Art. 2 (2016), rec.13; Barlag, in: Roßnagel, DSGVO, Anwendungsbereich (2017), rec. 12.

[31]Plath, in: Plath, BDSG/DSGVO, Art. 2 (2016), rec. 14.

activity irrespective of whether it is remunerated, as well as preparatory measures for the former, such as marketing measures or trading personal data for receiving a service.[32]

Example

According to the ECJ, the operation of a surveillance camera, where the recorded video material is stored on a continuous recording device, installed by an individual on his family home for the purposes of protecting the property, health and life of the home owners, which also monitors a public space (such as a public street or sidewalk), does not constitute data processing in the course of a purely personal or household activity.[33]

Controllers or processors that provide the means for personal data processing under this provision cannot benefit from this exemption.[34]

2.2 To Whom Does the Regulation Apply?

The GDPR applies to anyone *processing or controlling* the processing of personal data. Given the economic importance of data, especially companies will be affected by the GDPR. As the *legal form* of the entity is irrelevant, there is a great variety of norm addressees. The different parties falling within the scope of application of the GDPR are provided by the latter with different roles and obligations for data security. In order to establish the personal scope of application of the GDPR and the resulting data protection responsibilities, it must therefore be determined who is a 'controller', who is a 'processor' and who benefits from data protection under the GDPR.

2.2.1 'Controller'

A 'controller' is a natural or legal person, public authority, agency or other body that, alone or jointly with others, determines the purposes and means of the processing of personal data, Art. 4 No. 7 GDPR. The definition is identical with the one in the Data Protection Directive. Thus, the legal definition consists of *three main components*: (1) a natural or legal person, public authority, agency or other body (2) that alone or jointly with others (3) determines the purposes and means of data processing.

[32]Ernst, in: Paal/Pauly, DSGVO, Art. 2 (2017), rec. 19.

[33]ECJ, ruling of 11 December 2014, František Ryneš./.Úřad pro ochranu osobních údajů, C-212/13, rec. 35.

[34]Rec. 18 GDPR.

2.2.1.1 Natural or Legal Person, Public Authority, Agency or Other Body. . .

The *legal form* of the controller is not decisive for being considered responsible for the legal obligations under the GDPR. Company groups should be aware of the fact that the GDPR does not provide for an intra-group exemption. Each company within a group structure is solely responsible for the data processing taking place under its controllership (see Sect. 4.4). As a consequence, each entity is deemed a controller.

Internally, relevant decisions will be taken by the managing director(s) or the management board of a (stock) company. Nevertheless, as they act on behalf of the company, the latter shall be deemed controller.[35] This is preferable in the strategic perspective of liability and impending fines for providing data subjects with a more stable and reliable reference entity for the exercise of their rights.[36]

Nevertheless, it cannot be entirely excluded that the individuals taking decisions for a legal entity might be deemed controllers based on the circumstances of the individual case. This would be the case where the individual acting within the legal entity uses personal data for its own purposes outside of the scope and possible control of the entity's activities.[37]

2.2.1.2 Alone or Jointly with Others. . .

The legislator was aiming for a clear allocation of responsibilities and therefore introduced the concept of *joint controllers* in Art. 26 GDPR. If the purpose and means of the processing are determined by various entities together, those entities will share data protection obligations under the GDPR and have to cater for a clear allocation of responsibilities. Joint controllership may take *different forms*: the relevant entities might have a very close relationship (e.g., sharing all purposes and means of a processing) or a more lose relationship (e.g., partially sharing purposes).[38] For detailed information and examples, see Sect. 3.2.2.

In this context, it is important to differentiate between controllers and processors. As just shown, joint control can take a broad variety of forms and multiple parties may interact or be linked with each other when it comes to processing personal data.[39] Until the creation of the GDPR, the concept of joint controllership was only mentioned but not defined by law and was therefore *rarely used* in practice. Faced with multiple actors, Supervisory Authorities, courts and academics would rather presume a case of commissioned data processing (in other words, one controller delegating tasks to one or several processors).[40] This situation is very *likely to change*, given the legislative introduction of this concept.

[35] See also Art. 29 Data Protection Working Party, WP 169 (2010), pp. 15–16.

[36] See also Art. 29 Data Protection Working Party, WP 169 (2010), p. 15; Wybitul/Schultze-Melling, Datenschutz (2014), recs. 72–73.

[37] See also Art. 29 Data Protection Working Party, WP 169 (2010), p. 16.

[38] See also Art. 29 Data Protection Working Party, WP 169 (2010), p. 19.

[39] See also Art. 29 Data Protection Working Party, WP 169 (2010), p. 19.

[40] Dovas, ZD 2016, 512, 514.

The following criteria can help to differentiate between controller and processor and suggest that the entity in question, carrying out the data processing on behalf of a contracting party, is a *controller* rather than a processor based on its influence on the purposes and/or means of processing[41]:

- *freedom from instructions* by the contracting entity that delegated the data processing to the processing entity in question;
- *merging* of the data received upon delegation with own databases;
- use of the data for *own purposes* that may have not been agreed upon with the contracting entity;
- processed data having been collected by way of a *legal relationship* between the processing entity and the data subjects;
- *responsibility* of the processing entity for the lawfulness and accuracy of the data processing.

2.2.1.3 Determines the Purposes and Means of the Processing of Personal Data. . .

Controllership depends not upon the execution of data processing but upon *decision-making power*. The relevant questions are: why does the processing take place, and who initiated it?[42] Whilst the controller is entitled to decide upon the purpose of processing and its essential elements, the technical and organisational means of processing can—at least partially—be delegated to someone else. In greater detail, this means that the controller has to choose, inter alia, which data shall be processed, for how long, who shall have access and what security measures need to be taken. Less crucial matters, such as the choice of the hard- or software, do not necessarily have to be specified by the controller.[43]

Decision-making power as to data processing can result from an *explicit or implicit legal responsibility* or from an *actual influence* as to the purposes and means of processing[44]:

- Explicit legal responsibility arises for public authorities by way of legislation establishing their fields of competence (such as administrative law). Implicit legal responsibility stems from common legal provisions or established legal practice pertaining to different areas (civil law, commercial law, labour law, . . .),

[41]Criteria drawn from v.d.Bussche/Voigt, in: v.d.Bussche/Voigt, Konzerndatenschutz, Auftragsdatenverarbeitung (2014) recs. 22–26; Gola/Wronka, Arbeitnehmerdatenschutz (2013), rec. 277.

[42]See also Art. 29 Data Protection Working Party, WP 169 (2010), p. 8.

[43]See also Art. 29 Data Protection Working Party, WP 169 (2010), p. 14 et seq.

[44]Laue/Nink/Kremer, Datenschutzrecht, Einführung (2016), recs. 48–52; see also Art. 29 Data Protection Working Party, WP 169 (2010), pp. 10–12, 14.

such as the employer in relation to data on its employees, the association in relation to data on its members or contributors.
– Actual influence will usually be established by assessing the contractual relations between the different parties involved, which will allow for drawing external conclusions, assigning the role and responsibilities of controller to one or more parties.

2.2.2 'Processor'

In addition to the controller, the Regulation imposes data protection obligations on the 'processor'. The latter is defined as a natural or legal person, public authority, agency or other body that processes personal data *on behalf* of the controller, Art. 4 No. 8 GDPR. Thus, the existence of a processor depends on a *decision taken by the controller*, who can either process data within its organisation (e.g., through its own employees) or delegate all or part of the processing activities to an external organisation, rendering the latter a 'processor'.[45] Two conditions have to be met to qualify as a 'processor':

– being a *separate* legal entity/individual with respect to the controller; and
– processing personal data *on behalf* of the controller.[46]

For example, processors could be *cloud computing* suppliers or computing centres.[47] As to its legal form, what has been said above concerning the controller also applies to the processor. Therefore, a broad variety of actors can be deemed processors. Also, several processors can be instructed to act at the same time. This, more and more often, happens in practice, whereas these processors may have a direct relationship with the data controller or be subcontractors to which the processors have delegated part of the processing activities entrusted to them.[48] Note, however, that any processor *exceeding his mission* and acquiring a relevant role in determining the purposes or essential means of data processing turns into a (joint) controller (see remarks in Sects. 2.2.1.2 and 3.2.2).[49]

2.2.3 Beneficiaries of Protection Under the GDPR

While the norm addressees of the GDPR have been specified above, the beneficiaries of data protection still need to be determined. The Regulation lays

[45] See also Art. 29 Data Protection Working Party, WP 169 (2010), p. 25.
[46] See also Art. 29 Data Protection Working Party, WP 169 (2010), p. 25.
[47] See also Gola/Klug/Körffer, in: Gola/Schomerus, BDSG, § 11 (2015), recs. 7–8.
[48] See also Art. 29 Data Protection Working Party, WP 169 (2010), p. 27.
[49] Art. 26 Sec. 10 GDPR; see also Art. 29 Data Protection Working Party, WP 169 (2010), p. 25.

down rules relating to the protection of *individuals*, Art. 1 Sec. 1 GDPR. Any individual, regardless of his nationality or place of residence, can beneficiate from protection under the GDPR.[50]

Specific Protection for Minors
Generally, all individuals regardless of their age benefit from protection under the GDPR. However, *children* benefit from specific, strengthened protection under the Regulation, as they may be less aware of the risks, consequences and safeguards concerned and their rights in the relation to the processing of personal data (see also Sect. 4.2.1.6).[51]

No Protection of Legal Persons
Legal entities do not benefit from protection under the GDPR, regardless of their legal form.[52] This is due to the fact that the legislator wanted to enforce the protection of individuals with regard to their fundamental rights under Art. 8 of the Charter of Fundamental Rights of the European Union and Art. 16 of the Treaty on the Functioning of the European Union (TFEU).[53] However, the data of legal persons could be deemed personal data under the GDPR if it contains information on the *individuals associated* with the legal person, e.g., information on a persons' share or function in a company.[54] Moreover, as regards legal persons, there is an exception: the *one-man-owned entity* is viewed as a natural person because it is not possible to separate personal and corporate data in this situation.[55]

2.3 Where Does the Regulation Apply?

Article 3 – 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

[50]Rec. 14 GDPR.
[51]Rec. 38 GDPR.
[52]Rec. 14 Data Protection Directive.
[53]Rec. 1 GDPR.
[54]Ernst, in: Paal/Pauly, DSGVO, Art. 4 (2017), rec. 5; see also Dammann, in: Simitis, BDSG, § 3 (2014), recs. 19, 44.
[55]Blume, EDPL 2015, 258, 258.

(b) the monitoring of their behaviour as far as their behaviour takes place within the Union.

3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.

Although the GDPR is a European Regulation, its territorial scope does not stop at European boundaries. Given a global economy with multinational groups and cross-border data transfer, international aspects have been taken into consideration upon creation of the GDPR. *Transnational application* shall guarantee comprehensive privacy of individuals and fair competitive conditions on the EU internal market. Also, the phenomenon of *forum shopping* shall be prevented: due to the different data protection standards within the EU Member States, companies could choose their place of business according to the lowest national level of data protection standards (among other factors). Thus, EU legislation prescribes a particularly broad territorial scope.[56]

From a territorial perspective, the GDPR does not differentiate between controller and processor and sets out the same *territorial scope* for both of them. Mainly, the GDPR applies in the following two situations[57]:

- the processing of personal data takes place *in the context of the activities of an establishment* of the controller or processor *within the EU*; or
- the *processing of the data of individuals within the EU* takes place by a controller or processor not established in the EU.

2.3.1 Data Processing in the Context of the Activities of an EU Establishment

According to Art. 3 Sec. 1 GDPR, the GDPR is applicable to processing of personal data in the context of the activities of an establishment of a controller or processor in the EU, regardless of whether the processing takes place in the EU or not. The provision applies the *establishment principle*, according to which the choice of law depends on where an entity is established. For the applicability of the GDPR, it is therefore not necessarily decisive where the data is being processed.

2.3.1.1 Flexible Concept of Establishment

Establishment implies the effective and real exercise of activity through stable arrangements.[58]

[56]ECJ, ruling of 13 May 2014, Google Spain, C-131/12, rec. 54.

[57]Besides, the GDPR applies to data processing within diplomatic or consular representations of a Member State, Art. 3 Sec. 3 GDPR.

[58]Rec. 22 GDPR.

Stable arrangements are not determined by their legal form; it does not matter whether the relevant body is a branch or a subsidiary company with legal personality.[59] Also, the place of registration does not automatically equate the place of establishment but the former might be an indication for the latter.[60] To ensure a high level of protection of personal data, the term 'establishment' cannot be interpreted restrictively.[61] The degree of *stability* of an arrangement needs to be determined according to the nature of its economic activities and the services offered.[62] Both elements of the definition have to be interpreted in connection with each other. Even the presence of one representative within a Member State can suffice to constitute an establishment if said representative provides his services with a certain degree of stability.[63] The existence of an 'establishment' depends on the *individual circumstances* of the case. Even having a bank account or a post office box in a Member State could constitute a stable arrangement.[64]

The stability must be determined in connection with the specific nature of the activity, e.g., if a company offers services exclusively over the Internet.[65] In the latter case, the existence of an arrangement that is involved in offering or administrating such services in an EU Member State might qualify as 'establishment'.[66] Both the stability of the arrangements and the activity's contribution to the data processing need to be balanced out. The economic activity within the stable arrangements can ultimately be a minor one, e.g., running a website for offering services.[67] Thus, both human or material resources might qualify as 'stable arrangement'.

Example

A non-EU entity has a bank account, a post office box and a representative in an EU Member State that serves as exclusive contact point for the customers in said EU Member State.[68]

In this example, the human and material resources of the entity in the EU Member State should qualify as stable arrangements and, thus, an establishment.

[59]Rec. 22 GDPR.

[60]ECJ, ruling of 1 October 2015, Weltimmo, C-230/14, rec. 29.

[61]ECJ, ruling of 13 May 2014, Google Spain, C-131/12, rec. 53.

[62]ECJ, ruling of 1 October 2015, Weltimmo, C-230/14, rec. 29.

[63]Barlag, in: Roßnagel, DSGVO, Anwendungsbereich (2017), rec. 16; ECJ, ruling of 1 October 2015, Weltimmo, C-230/14, rec. 30.

[64]Plath, in: Plath, BDSG/DSGVO, Art. 3 (2016), rec. 8.

[65]ECJ, ruling of 1 October 2015, Weltimmo, C-230/14, rec. 29.

[66]Kartheuser/Schmitt, ZD 2016, 155, 158.

[67]ECJ, ruling of 1 October 2015, Weltimmo, C-230/14, rec. 31 et seq.

[68]ECJ, ruling of 1 October 2015, Weltimmo, C-230/14.

2.3.1.2 Processing 'in the Context of the Activities'

As data processing only needs to take place 'in the context of the activities' of the establishment, the latter does not have to carry out any data processing activities itself.[69] To fall within the territorial scope of application of the GDPR, it is sufficient if the establishment *economically supports* the data processing carried out by the mother company, e.g., through selling and promoting advertising space offered by a search engine in order to make its services profitable.[70] Ultimately, there has to be a connection between the economic activity of the establishment and the data processing.[71]

As just shown, the geographic execution of the actual processing—whether within or outside the EU—is not decisive for establishing the applicability of the GDPR under this provision.[72]

Example

A non-EU entity has an office in an EU Member State that does not carry out any processing activities itself but develops customer relationships and acquires a considerable number of clients for the entity and, thus, has a large share in the economic success of the entity.

In this example, the entity's EU-located office develops customer relationships and, thus, has a considerable degree of stability that qualifies the office as 'establishment'. Even though said establishment does not carry out any processing activities, it majorly contributes to the entity's economic success, and thus based on the ECJ's jurisprudence in the 'Google Spain' case, the GDPR applies to the non-EU entity.[73]

2.3.1.3 Important Cases of Application

Based on the above, Art. 3 Sec. 1 GDPR applies to a large variety of situations and potentially affects companies outside the EU.

Example

An EU Entity Processes and Collects Personal Data Itself

Entity A is a winemaker located in France that delivers its products to all EU Member States. For this purpose, A runs not only a local shop in Paris but also an online shop. Names and addresses of the customers are stored as contact information in order to carry out wine deliveries.

[69] ECJ, ruling of 13 May 2014, Google Spain, C-131/12, rec. 52; Plath, in: Plath, Art. 3 (2016), rec. 9.

[70] ECJ, ruling of 13 May 2014, Google Spain, C-131/12, rec. 55; Plath, in: Plath, Art. 3 (2016), rec. 9.

[71] ECJ, ruling of 13 May 2014, Google Spain, C-131/12, rec. 52.

[72] Laue/Nink/Kremer, Datenschutzrecht, Einführung (2016), rec. 79, see also for the following example.

[73] ECJ, ruling of 13 May 2014, Google Spain, C 131/12.

In this example, A is controller of the processing of personal data (collected in the EU) as it stores customer data. A has its sole establishment in France. Thus, A is carrying out the data processing of its customer data in the context of the activities of its French (and thus EU) establishment and falls within the scope of application of the GDPR.

Example

An EU Entity Collects Personal Data in One EU Member State and Uses a Processor in Another EU Member State

Entity B is an Italian airline operating flights across Europe. Flight tickets can only be booked online. In order to successfully carry out the booking process, customer data needs to be processed and stored. As B has a large customer base, it accumulates a large amount of customer data. Therefore, B stores the customer data in a cloud service operated by Spanish entity C. The purposes and means of the processing are determined by B.

In this example, B is a controller established in Italy. The processing is carried out through C that is established in Spain, whereas the purposes and means of processing are determined by B. Thus, C acts as a processor. Both the controller and processor are established in the EU (in different EU Member States). As they carry out their activities in the context of their EU establishments, the GDPR applies to B and to C.

Example

An EU Entity Carries Out Data Processing Through a Non-EU Entity

Entity E is a German personnel service provider that assigns temporary employees to large automobile manufacturers throughout Europe. Due to its large and constantly changing pool of employees, E stores the data from the application processes in a cloud service operated by US entity F. The purpose and means of the processing are determined by E.

In this example, E is a controller established in Germany. F is a processor operating in the US. The GDPR applies to E since E is a controller established within the EU and processing takes place in the context of its activities (= providing personnel services within Europe). As for F, the GDPR would only be applicable if F itself targets the European market with its activities (Art. 3 Sec. 2 GDPR). In any case, E needs to bind F by contract to adhere to the data protection standards of the GDPR in order to fulfil its own data protection obligations under the Regulation.

2.3.2 Processing of Personal Data of Data Subjects in the EU

If neither controller nor processor is established within the EU, the GDPR can apply nevertheless. In order to ensure that individuals are not deprived of their data protection rights, the EU legislator extended the territorial scope of application of European data protection law by introducing the principle of *lex loci solutionis* in Art. 3 Sec. 2 GDPR. According to this principle, the applicable law depends on where the relevant *contractual performance* is being offered. Broadly speaking, it is decisive where the contractual offer occurs. Article 3 Sec. 2 GDPR will therefore affect entities that *target* consumers in the *EU internal market*. Companies should keep in mind that the nationality of their customers is irrelevant as long as they are located in the EU (as shown previously in Sect. 2.2.3). Furthermore, they might have to appoint an EU representative (see Sect. 4.3.8) as contact point for data subjects and Supervisory Authorities within the EU.

2.3.2.1 Offering of Goods or Services to Data Subjects in the EU

According to Art. 3 Sec. 2 lit. a GDPR, data processing that is related to the offering of goods or services in the EU, irrespective of whether a payment by the latter is required, falls within the territorial scope of application of the GDPR. This will primarily affect international corporations offering services via the Internet.[74] In order to determine whether goods or services are targeted towards the internal market, it should be ascertained whether the controller or processor specifically envisages offering services in one or more EU Member States.[75] For example, an Australian company does not necessarily address its goods or services to individuals in England or Scotland just because its website is available in English. The company in question must intend to *address European consumers*. The mere accessibility of a website, an email address or other contact details or the use of a language generally used in the third country where the company is established is insufficient to ascertain such intention.[76] However, *indices* for targeting EU individuals could be as follows[77]:

- the use of a language generally used in one or more EU Member States; or
- the accepted currencies (especially the Euro); or
- the mentioning of customers or users from Europe; or
- the possibility of delivery to one or more Member States; or
- the domain name of the website referring to one or more EU Member State (s) ('xxx.com/de', 'xxx. es', . . .).

[74]Barlag, in: Roßnagel, DSGVO, Anwendungsbereich (2017), rec. 18.

[75]Rec. 23 GDPR.

[76]Rec. 23 GDPR.

[77]The following examples are (partially) drawn from rec. 23 GDPR; ECJ, ruling of 7 December 2010, Alpenhof, joined cases C-585/08 and C-144/09, recs. 80–84.

Example

A Non-EU Based Entity Offers Goods in EU Member States

Entity H is located in Australia and runs an online shop. The company has no subsidiaries or representatives abroad and the online shop is available in English only. H stores the customer data. Payment is accepted in Australian dollars, as well as euros, and deliveries are possible to Germany, France and Italy. If customers from those EU Member States call up H's website, they are redirected from the domain 'H.au' to 'H.com/de', 'H.com/fr' and so forth.

In this example, the separate domain name for European customers, the possibility of payment in euro and the possibility to deliver to certain EU Member States allow the conclusion that H addresses customers located in the EU. Therefore, the GDPR applies.

Example

A Non-EU Entity Offers Services in EU Member States

Entity I is located in the US and runs a portal for peer-to-peer holiday apartment rental. Via I's website, customers from around the world can rent out their apartments to tourists. In order to offer an apartment on I's website, each person needs to open a user account and enter a number of details, such as the name and the address of the apartment. I stores this user data. If a person calls up the website, it will be redirected to a website corresponding to its IP geolocation data. If, for example, the user selects 'France', the website appears in French language and the domain name changes from 'I.com' to 'I.com/fr'. Rental prices will then be indicated in euro instead of US dollar.

In this example, different indices imply that I is addressing persons located in the EU: the possibility to change the language and the currency shown on the website to the ones of EU Member States and the domain name(s) suggest that I (also) addresses customers located in the EU. Therefore, the GDPR applies.

2.3.2.2 Monitoring of EU Customers' Behaviour

According to Art. 3 Sec. 2 lit. b GDPR, data processing that is related to the monitoring of EU customers' behaviour, as far as their behaviour takes place within the Union, falls within the territorial scope of application. In order to determine if behaviour qualifies as 'monitoring' under this article, it should be ascertained whether individuals are tracked on the Internet, including potential subsequent use of personal data processing techniques that consist of *profiling* an individual.[78] This is particularly the case if processing takes place in order to take decisions concerning that individual or for analysing or predicting the persons' preferences, behaviours and attitudes.[79]

[78] Rec. 24 GDPR.

[79] Rec. 24 GDPR.

In short, any form of *web tracking* will be deemed monitoring, such as via cookies or social media plug-ins.[80] Web tracking tools allow website providers to analyse the behaviour of the website's users, e.g., by measuring how long, how often or on what way (e.g., through a search engine or online advertising) the website was visited. Usually, the analytic tool will store a *cookie* that contains a unique ID on the website user's computer. This ID will be used by the tool to identify the browser every time the user visits the website and, subsequently, to analyse his behaviour. Profiling can take place in various different forms and via different tools. In this regard, it should be noted that, even without cookies, a user's browser might allow website providers to identify users and monitor their behaviour: each browser inevitably transfers a number of data when accessing a website to the provider in order to enable an optimised display of said website, such as type and version of the browser, the operating system, installed plug-ins (e.g., flash plug-in), language, header and cookie settings, the used monitor resolution and time zone.[81] These data allow the provider to generate a unique *browser fingerprint* that might, combined with additional information such as IP addresses, permit identifying users when they access said website again.[82]

Example

Entity J is located in Hong Kong and sells trend-oriented furniture and home accessories online. The products can only be paid in US dollar, and delivery to Europe is not offered. However, J wants to analyse the European market as it is considering expanding its business. Anyone calling up the website needs to accept the usage of cookies, and J analyses the IP geolocation data to determine the country where the user is located. J processes the obtained data in order to find out how many European customers from which Member States visit the website and what they are mainly interested in.

In this example, J is using web tracking to analyse the preferences of customers located in the EU. Therefore, the GDPR applies.

2.3.2.3 Time of Stay of the Data Subject in the EU

Given a global economy, characteristics like nationality or place of residence become less important for the scope of data protection and the *place where a person stays* becomes decisive. As Art. 3 Sec. 2 GDPR refers to data subjects 'in the EU' or their behaviour taking place 'within the EU', it needs to be clarified at what point in time the data subject must be present in the EU for the applicability of the GDPR. The wording of Art. 1 Sec. 1 GDPR does not provide for details as to which time is decisive for determining whether a person is staying in the EU and therefore merits protection under the GDPR. One option would be that the time of

[80] Schantz, NJW 2016, 1841, 1842; Hornung, ZD 2012, 99, 102.
[81] Alich/Voigt, CR 2012, 344, 345.
[82] Alich/Voigt, CR 2012, 344, 346–347.

the data processing is decisive.[83] As a consequence, an EU resident going on vacation to, e.g., the US would not benefit from protection under the GDPR for the time of his trip.[84] As this option does not seem to meet the legislator's intention to maximise data protection, it seems to be the more likely option that *the time of the collection* (in a broad sense) of the data is decisive.[85] This way, all following steps of data processing will have to meet the standards set out by the GDPR.[86]

References

Albrecht JP (2016) Das neue EU-Datenschutzrecht – von der Richtlinie zur Verordnung. CR, pp 88–98

Alich S, Voigt P (2012) Mitteilsame Browser – Datenschutzrechtliche Bewertung des Trackings mittels Browser-Fingerprints. CR, pp 344–348

Art. 29 Data Protection Working Party (2007) Opinion 4/2007 on the concept of personal data, WP136

Art. 29 Data Protection Working Party (2010) Opinion 5/2014 on Anonymisation Techniques, WP216

Art. 29 Data Protection Working Party (2014) Opinion 1/2010 on the concepts of 'controller' and 'processor', WP 169

Barlag C (2017) Anwendungsbereich der Datenschutz-Grundverordnung. In: Roßnagel A (ed) Europäische Datenschutz-Grundverordnung, Vorrang des Unionsrechts – Anwendbarkeit des nationalen Rechts, 1st edn. Nomos, Baden-Baden

Bergt M (2015) Die Bestimmbarkeit als Grundproblem des Datenschutzrechts – Überblick über den Theorienstreit und Lösungsvorschlag, pp 365–371

Blume P (2015) The data subject. EDPL 4:258–264

Buchner B (2016) Grundsätze und Rechtmäßigkeit der Datenverarbeitung unter der DS-GVO. DuD, pp 155–161

Dammann U (2014) § 3 BDSG. In: Simitis S (ed) Bundesdatenschutzgesetz, 8th edn. Nomos, Baden-Baden

Dovas M-U (2016) Joint Controllership – Möglichkeiten oder Risiken der Datennutzung? ZD, pp 512–517

Ernst S (2017) Arts. 2, 4 DSGVO. In: Paal BP, Pauly DA (eds) Beck'sche Kompaktkommentare Datenschutz-Grundverordnung, 1st edn. C.H. Beck, Munich

Gola P, Wronka G (2013) Handbuch zum Arbeitnehmerdatenschutz, 6th edn. Frechen, DATAKONTEXT GmbH

Gola P, Klug C, Körffer B (2015) § 11 BDSG. In: Gola P, Schomerus R (eds) Bundesdatenschutzgesetz Kommentar, 12th edn. C.H. Beck, Munich

Herbst T (2016) Was sind personenbezogene Daten? NVwZ, pp 902–906

Hornung G (2012) Eine Datenschutz-Grundverordnung für Europa? – Licht und Schatten im Kommissionsentwurf vom 25.1.2012. ZD, pp 99–106

Kartheuser I, Schmitt F (2016) Der Niederlassungsbegriff und seine praktischen Auswirkungen. ZD, pp 155–159

Laue P, Nink J, Kremer S (eds) (2016) Einführung. In: Das neue Datenschutzrecht in der betrieblichen Praxis, 1st edn. Nomos, Baden-Baden

[83] Albrecht, CR 2016 88, 90; Plath, in: Plath, BDSG/DSGVO, Art. 3 (2016), rec. 14.

[84] Plath, in: Plath, BDSG/DSGVO, Art. 3 (2016), rec. 14.

[85] Arguing in this direction is Plath, in: Plath, BDSG/DSGVO, Art. 3 (2016), rec. 14.

[86] Plath, in: Plath, BDSG/DSGVO, Art. 3 (2016), rec. 14.

Piltz C (2016) Die Datenschutz-Grundverordnung. K&R, pp 557–567
Plath K-U (ed) (2016) Arts. 2, 3 DSGVO. In: BDSG/DSGVO, 2nd edn. Verlag Dr. Otto Schmidt, Cologne
Schantz P (2016) Die Datenschutz-Grundverordnung – Beginn einer neuen Zeitrechnung im Datenschutzrecht. NJW, pp 1841–1847
Schild HH (2016) Art. 4 DSGVO. In: Wolff HA, Brink S (eds) Beck'scher Online-Kommentar Datenschutzrecht, 18th edn. C.H. Beck, Munich
Schreiber L (2016) Art. 4 DSGVO. In: Plath K-U (ed) BDSG/DSGVO, 2nd edn. Verlag Dr. Otto Schmidt, Cologne
Voigt P (2009) Datenschutz bei Google. MMR, pp 377–382
von dem Bussche AF, Voigt P (eds) (2014) Auftragsdatenverarbeitung im Konzern. In: Konzerndatenschutz Rechtshandbuch, 1st edn. C.H. Beck, Munich
Wybitul T, Schultze-Melling J (2014) Datenschutz im Unternehmen: Handbuch, 2nd edn. Fachmedien Recht und Wirtschaft, Frankfurt am Main

Organisational Requirements

3

The GDPR introduces an extended liability and increased penalties (see Chap. 7). With this in mind, companies should be particularly careful when adjusting their data protection measures to meet the increased protection standards. Many companies will have to make a considerable effort in order to implement a Data Protection Management System (DPMS) that complies with the Regulation. However, the harmonisation across the EU also facilitates the data protection organisation for international corporations.

The GDPR is following a *risk-based approach* on data security. The following sections provide information on the organisational requirements imposed by the GDPR upon controllers and—to a lesser extent—processors.

3.1 Accountability

Whereas the former Data Protection Directive did not explicitly emphasise on accountability, the GDPR introduces the general *principle of accountability* in Art. 5 Sec. 2 GDPR, which imposes the *responsibility for the compliance* of processing with the GDPR and the *burden of proof* for said compliance onto the *controller*.

Thus, the principle of accountability consists of two elements:

1. the *responsibility* of the controller to *ensure compliance* with the GDPR; and
2. the controller's *ability to prove compliance* to Supervisory Authorities.

Responsibility to Ensure Compliance

The general accountability principle is *directly enforceable* and can be fined with up to EUR 20,000,000.00 or up to 4% of the total worldwide annual turnover (Art. 83 Sec. 5 lit. a GDPR; see Sect. 7.3). The impending fines shall increase the pressure on controllers to implement appropriate measures for data protection. The principle is further specified by the different material and organisational

P. Voigt, A. von dem Bussche, *The EU General Data Protection Regulation (GDPR)*,
DOI 10.1007/978-3-319-57959-7_3