

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

© Springer International Publishing AG 2017

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, express or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

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

1	Introduction and ‘Checklist’	1
1.1	Legislative Purpose and Previous Legal Provisions	1
1.1.1	The Data Protection Directive	1
1.1.2	The General Data Protection Regulation	2
1.2	Checklist: Most Important Data Protection Obligations	3
1.2.1	Organisational Requirements	3
1.2.2	Lawfulness of the Processing Activities	5
	References	7
2	Scope of Application of the GDPR	9
2.1	In Which Case Does the Regulation Apply?	9
2.1.1	‘Processing’	9
2.1.2	‘Personal Data’	11
2.1.3	Exemptions from the Scope of Application	16
2.2	To Whom Does the Regulation Apply?	17
2.2.1	‘Controller’	17
2.2.2	‘Processor’	20
2.2.3	Beneficiaries of Protection Under the GDPR	20
2.3	Where Does the Regulation Apply?	21
2.3.1	Data Processing in the Context of the Activities of an EU Establishment	22
2.3.2	Processing of Personal Data of Data Subjects in the EU	26
	References	29
3	Organisational Requirements	31
3.1	Accountability	31
3.2	General Obligations	33
3.2.1	Responsibility, Liability and General Obligations of the Controller	33
3.2.2	The Allocation of Responsibility Between Joint Controllers	34
3.2.3	Cooperation with Supervisory Authorities	37
3.3	Technical and Organisational Measures	38
3.3.1	Appropriate Data Protection Level	38

3.3.2	Minimum Requirements	39
3.3.3	Risk-Based Approach Towards Data Security	40
3.3.4	The NIS Directive	42
3.4	Records of Processing Activities	44
3.4.1	Content and Purpose of the Records	44
3.4.2	Exemption from the Obligation to Maintain Records	45
3.5	Data Protection Impact Assessment	47
3.5.1	Affected Types of Data Processing	47
3.5.2	Scope of the Assessment	49
3.6	Data Protection Officer	53
3.6.1	Designation Obligation	53
3.6.2	Aspects Regarding the Designation of the Data Protection Officer	56
3.6.3	Position	58
3.6.4	Responsibilities	60
3.7	Privacy by Design and Privacy by Default	62
3.8	Personal Data Breaches	65
3.8.1	Personal Data Breach	65
3.8.2	Notification to the Supervisory Authority	65
3.8.3	Communication to the Data Subjects	69
3.9	Codes of Conduct, Certifications, Seals, Etc.	71
3.9.1	Relationship Between Codes of Conduct and Certifications	71
3.9.2	Codes of Conduct	72
3.9.3	Certifications, Seals, Marks	77
3.10	Data Processors	80
3.10.1	Privileged Position of the Processor	80
3.10.2	Obligation of the Controller When Choosing a Processor	81
3.10.3	Obligations of the Processor	83
3.10.4	Designation of a Sub-Processor	84
	References	84
4	Material Requirements	87
4.1	Basic Principles	87
4.1.1	Lawfulness, Fairness and Transparency	88
4.1.2	Purpose Limitation	88
4.1.3	Data Minimisation	90
4.1.4	Accuracy	91
4.1.5	Storage Limitation	92
4.1.6	Integrity and Confidentiality	92
4.2	Legal Justifications for Data Processing	92
4.2.1	Processing Based on Consent	93
4.2.2	Processing Based on a Legal Permission	100
4.2.3	Processing of Special Categories of Personal Data	110

4.3	Data Transfers to Third Countries	116
4.3.1	Safe Third Countries	117
4.3.2	Consent	118
4.3.3	Standard Contractual Clauses	119
4.3.4	EU–U.S. Privacy Shield	122
4.3.5	Binding Corporate Rules	125
4.3.6	Codes of Conduct, Certifications, Etc.	129
4.3.7	Derogations for Specific Situations	130
4.3.8	Appointment of a Representative by Non-EU Entities	133
4.4	Limited Privilege for Intra-Group Processing Activities	135
4.4.1	Separate Data Protection Responsibility of Each Group Member	136
4.4.2	Facilitations Regarding Material Requirements	137
4.4.3	Facilitation Regarding Organisational Requirements	138
	References	138
5	Rights of Data Subjects	141
5.1	Transparency and Modalities	141
5.1.1	The Manner of Communicating with the Data Subject	142
5.1.2	The Form of Communication	143
5.2	Information Obligation of the Controller Prior to Processing	143
5.2.1	Time of Information	144
5.2.2	Collection of the Data from the Data Subject	144
5.2.3	Obtainment of the Data from Another Source	146
5.2.4	Practical Implications	147
5.3	Response to Data Subjects’ Requests	147
5.3.1	Manner of Response	147
5.3.2	Time of Response	149
5.3.3	Information in Case of Inaction	149
5.3.4	Verification of the Data Subject’s Identity	150
5.4	Right to Access	150
5.4.1	Scope of the Right to Access	150
5.4.2	Provision of Access to the Personal Data	152
5.4.3	Practical Implications	153
5.5	Rights to Erasure, Rectification and Restriction	154
5.5.1	Right to Rectification	154
5.5.2	Right to Erasure	156
5.5.3	Right to Restriction of Processing	164
5.5.4	Notification of Third Parties Regarding the Rights to Erasure, Rectification and Restriction, Art. 19	167
5.6	Right to Data Portability	168
5.6.1	Scope and Exercise of the Right to Data Portability	169
5.6.2	Technical Specifications	174
5.6.3	Transmission of the Data	174

5.6.4	Relation to the Right to Erasure	175
5.6.5	Exclusion of the Right to Data Portability	175
5.7	Right to Object	176
5.7.1	Grounds for an Objection to Processing	177
5.7.2	Exercise of the Right and Legal Consequences	179
5.7.3	Information Obligation	180
5.8	Automated Decision-Making	180
5.8.1	Scope of Application of the Prohibition	181
5.8.2	Exceptions from the Prohibition	183
5.8.3	Appropriate Safeguards	184
5.9	Restrictions of the Data Subjects' Rights	184
	References	185
6	Interaction with the Supervisory Authorities	189
6.1	Determination of the Competent Supervisory Authority	189
6.2	One-Stop-Shop Mechanism	191
6.3	Determination of the Competent Lead Supervisory Authority	192
6.3.1	Determination Based on an Entity's Main Establishment	192
6.3.2	Determination in the Absence of an EU Establishment	195
6.3.3	Exception: Local Competences	195
6.4	Cooperation and Consistency Mechanism	197
6.4.1	European Data Protection Board	197
6.4.2	Cooperation Mechanism	198
6.4.3	Consistency Mechanism	198
	References	199
7	Enforcement and Fines Under the GDPR	201
7.1	Tasks and Investigative Powers of the Supervisory Authorities	201
7.1.1	Greater Consistency of Investigative Powers Throughout the EU	202
7.1.2	Scope of Investigative Powers	202
7.1.3	Exercise of the Powers	204
7.2	Civil Liability	204
7.2.1	Right to Claim Compensation	205
7.2.2	Liable Parties	207
7.2.3	Exemption from Liability	208
7.3	Administrative Sanctions and Fines	208
7.3.1	Corrective Powers of the Supervisory Authorities	209
7.3.2	Grounds for and Amounts of Administrative Fines	210
7.3.3	Imposition of Fines, Including Mitigating Factors	211
7.3.4	Sanctioning of Groups of Undertakings	212
7.3.5	Practical Implications	213

7.4	Judicial Remedies	214
7.4.1	Remedies Available to Data Processing Entities	214
7.4.2	Remedies Available to Data Subjects	215
	References	216
8	National Peculiarities	219
8.1	Various Opening Clauses	219
8.1.1	Opening Clauses Included in General Provisions of the GDPR	219
8.1.2	EU Member State Competence for Specific Processing Situations	223
8.2	Employee Data Protection	224
8.2.1	Opening Clause	225
8.2.2	Co-determination Bodies Provided for in Selected EU Member States	226
8.3	Telemedia Data Protection	230
	References	232
9	Special Data Processing Activities	235
9.1	Big Data	235
9.1.1	Applicability of the GDPR	236
9.1.2	Accountability	237
9.1.3	Safeguarding the Basic Principles of Lawful Processing	237
9.2	Cloud Computing	238
9.2.1	Allocation of Responsibilities	239
9.2.2	Choosing a Suitable Cloud Service Provider	239
9.2.3	Third-Country Cloud Service Providers	240
9.3	Internet of Things	240
9.3.1	Legal Basis for Processing in the IoT	241
9.3.2	Privacy by Design and Privacy by Default	242
	References	242
10	Practical Implementation of the Requirements Under the GDPR	245
10.1	Step 1: ‘Gap’ Analysis	246
10.2	Step 2: Risk Analysis	246
10.3	Step 3: Project Steering and Resource/Budget Planning	247
10.4	Step 4: Implementation	247
10.5	Step 5: National Add-On Requirements	249
	References	249
	Annex I: Juxtaposition of the Provisions and Respective Recitals of the GDPR	251
	Index	381

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

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

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

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.

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

⁴Rec. 3 GDPR.

⁵Rec. 9 GDPR.

⁶Recs. 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 Kompaktcommentare 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

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

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

¹Rec. 15 GDPR.

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

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

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

⁵Rec.15 GDPR.

⁶Plath, 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 name⁸;
- 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 cookies⁹).

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

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

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

⁹Rec. 30 GDPR.

¹⁰Rec. 27 GDPR.

¹¹Ernst, 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.

¹²See 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.

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

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

¹⁵ECJ, 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.

¹⁶Such 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 following¹⁷:

- 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

¹⁷Rec. 26 GDPR.

¹⁸Piltz, K&R 2016, 557, 561.

¹⁹See also Art. 29 Data Protection Working Party, WP 136 (2007), p. 19 et seq.

²⁰Rec. 26 GDPR.

²¹See also Art. 29 Data Protection Working Party, WP 216 (2014), p. 12.

²²See also Art. 29 Data Protection Working Party, WP 216 (2014), p. 16.

²³Rec. 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 Advice²⁵

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*

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

²⁵See 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 Regulation²⁶:

- 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

²⁶Rec. 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 likelihood 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

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

²⁸Rec. 26 GDPR.

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

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

³¹Plath, 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.

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

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

³⁴Rec. 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 loose 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.

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

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

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

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

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

⁴⁰Dovas, *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 processing⁴¹:

- *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 processing⁴⁴:

- 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, . . .),

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

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

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

⁴⁴Laue/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

⁴⁵See also Art. 29 Data Protection Working Party, WP 169 (2010), p. 25.

⁴⁶See also Art. 29 Data Protection Working Party, WP 169 (2010), p. 25.

⁴⁷See also Gola/Klug/Körffer, in: Gola/Schomerus, BDSG, § 11 (2015), recs. 7–8.

⁴⁸See also Art. 29 Data Protection Working Party, WP 169 (2010), p. 27.

⁴⁹Art. 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 benefit 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

⁵⁰Rec. 14 GDPR.

⁵¹Rec. 38 GDPR.

⁵²Rec. 14 Data Protection Directive.

⁵³Rec. 1 GDPR.

⁵⁴Ernst, in: Paal/Pauly, DSGVO, Art. 4 (2017), rec. 5; see also Dammann, in: Simitis, BDSG, § 3 (2014), recs. 19, 44.

⁵⁵Blume, 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 situations⁵⁷:

- 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

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

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

⁵⁸Rec. 22 GDPR.