Contents

Chapter I – General provisions

Article 1

Subject-matter and objectives

1. This Regulation lays down rules relating to the protection of natural persons[1] with regard to the processing[2] of personal data[3] and rules relating to the free movement of personal data.

2. This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.[4]

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.[5]

Recitals:

(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) 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) Directive 95/46/EC of the European Parliament and of the Council 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 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.

(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.

(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.

(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 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.

(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.

(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.

(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 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.

(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.

(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.

(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.

(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.

Commentary:

1 See Art. 4 cmt. 1.

2 See Art. 4 No. 2 regarding the definition of the term "processing".

3 See Art. 4 No. 1 regarding the definition of the term "personal data". Cf. also Recital 14 sentence 2. The GDPR does not provide data protection for legal entities, as provided, for example, by the fundamental right to data protection under Austrian law. On this topic, please see CJEU 9 November 2010, C92/09 and C93/09 – Schecke. Please also see CJEU 10 December 2020, C-620/19, where the CJEU repeated that the GDPR only contains provisions for the protection of personal data of natural persons and not of data concerning legal entities and, thus, denied its competence (in the case at hand, a liquidator of a legal entity exercised the right of access pursuant to Art. 15 GDPR).

4 Cf. Art. 8 Charter ("Protection of personal data") and Art. 16 TFEU; cf. Recital 1.

5 As before under the Data Protection Directive, the GDPR does not only protect the **fundamental right of data protection**, but equally serves the purpose of implementing the **fundamental freedoms**. Therefore, exceeding the level of data protection set out in the GDPR by national laws continues to be problematic. Cf. in this regard CJEU 6 November 2003, C101/01 – *Lindqvist* and CJEU 24 November 2011, C468/10, C-469/10 – *ASNEF*.

Article 2

Material scope

1. This Regulation applies to the processing[1] of personal data[2] 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[3,4] or are intended to form part of a filing system.

2. This Regulation does not apply to the processing of personal data:

(a) in the course of an activity which falls outside the scope of Union law;[5]

(b) by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the TEU;[6]

(c) by a natural person in the course of a purely personal or household activity;[7]

(d) by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences, the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.[8]

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.[9]

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 to 15 of that Directive.[10]

Recitals:

(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 files, as well as their cover pages, which are not structured according to specific criteria should not fall within the scope of this Regulation.

(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.

(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 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 security. This is relevant for instance in the framework of anti-money laundering or the activities of forensic laboratories.

(20) While this Regulation applies, inter alia, 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.

(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 to 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.

Commentary:

1 Cf. Art. 4 No. 2 regarding the definition of the term "processing".

2 Cf. Art. 4 No. 1 regarding the definition of the term "personal data".

3 Cf. Art. 4 No. 6 regarding the definition of the term "filing system".

4 **Paper files** that are not structured according to specific criteria are not covered by the material scope of the GDPR. Recital 15 last sentence stipulates that "[f]iles or sets of files, as well as their cover pages, which are not structured according to specific criteria should not fall within the scope of this Regulation".

5 In particular, activities concerning **national security** are outside the scope of European Union law and, pursuant to Art. 2 para. 2 lit. a, therefore are not covered by the GDPR (see Recital 16; Art. 4 No. 2 TEU). However, the GDPR applies to the transfer of personal data for commercial purposes by a company in the EU to another company established in a third country, "irrespective of whether, at the time of that transfer or thereafter, that data is liable to be processed by the authorities of the third country in question for the purposes of public security, defence and State security" (CJEU 16 July 2020, C-311/18 – *Schrems II*, para. 89). In another decision, the CJEU ruled that Art. 2 para. 2 lit. a GDPR must be interpreted restrictively since it "constitutes an exception to the very wide definition of the scope of that regulation set out in Article 2(1) of that regulation" (CJEU 9 July 2020, C-272/19 para. 68).

6 Chapter 2 of Title V of the TEU mentioned in para. 2 lit. b refers to the **common foreign and security policy of the Union** (cf. Recital 16 sentence 2). The CJEU stated that the "fact that an activity is an activity characteristic of the State or of a public authority is not sufficient ground for that exception to be automatically applicable to such an activity", but that "it is necessary that that activity is one of the activities that are explicitly mentioned by that provision or that it can be classified in the same category as those activities" and thus, the CJEU ruled that the exception does not apply to the activities of the Petitions Committee of the Parliament of Land Hessen (CJEU 9 July 2020, C-272/19, para. 70).

7 The "household exemption" in para. 2 lit. c corresponds to Art. 3 para. 2 indent 2 Data Protection Directive. Recital 18 clarifies that "professional or commercial activity" is not covered by the term "personal activity". Recital 18 mentions further examples for "purely personal or household activities": (i) maintaining correspondence; (ii) holding of address directories; or (iii) the use of social

networking and online activity undertaken within the context of such personal or household activities. On the basis of the examples in Recital 18, the disclosure of personal data, as it is typically the case in social networks, may be out of scope of the GDPR. However, the exemption must be interpreted narrowly (cf. in particular CJEU 6 November 2003, C-101/01 – *Lindqvist*). As an example, the operation of a camera system, as a result of which a video recording of people is stored on a continuous recording device such as a hard disk drive, installed by an individual on his family home for the purposes of protecting the property, health and life of the home owners, but which also monitors a public space does not qualify as a "purely personal or household activity" (CJEU 11 December 2014, C-212/13 – *Ryneš*). The publication of personal data on a privately motivated but publicly available website is also not covered by the "household exemption" (cf. CJEU 11 November 2003, C101/01 – *Lindqvist*).

8 Data processing activities mentioned in para. 2 lit. d which are in particular stipulated in criminal procedure codes, criminal codes and police laws of the Member States are subject to Directive (EU) 2016/680 (cf. Recital 19).

9 See Recital 17. Regulation 45/2001 was repealed by Regulation 2018/1725 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data with effect from 11 December 2018. The reference to Regulation 45/2001 must be construed as reference to Regulation 2018/1725 (see Art. 99 sentence 2 of Regulation 2018/1725).

10 Since the GDPR is "without prejudice to" the **safe harbours** of Art. 12 to 15 E-Commerce-Directive, the provision of Internet access services (Art. 12), of caching services (Art. 13) or hosting services (Art. 14) will only be subject to criminal liability and/or liability for damages if the respective requirements are fulfilled. This applies in particular to damages pursuant to Art. 82, fines pursuant to Art. 83, and other penalties pursuant to Art. 84. Cf. also Recital 21.

Article 3

Territorial scope[1]

1. This Regulation applies to the processing of personal data in the context of the activities[2] of an establishment[3] of a controller or a processor[4] in the Union, regardless of whether the processing takes place in the Union or not.[5]

2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor[6] not established in the Union,[7] where the processing activities are related to:

(a) the offering of goods or services,[8] irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or

(b) the monitoring of their behaviour as far as their behaviour takes place within the Union.[9]

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.[10]

Recitals:

(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.

(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 controller envisages offering goods or services to data subjects in the Union.

(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.

(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.

Commentary:

1 Pursuant to Art. 4 Data Protection Directive (respectively pursuant to the data protection laws of the Member States), the Data Protection Directive generally applied to controllers if the data processing: (i) is carried out in the context of the activities of an establishment of the controller on the territory of the Member State (cf. Art. 4 No. 1 lit. a Data Protection Directive); or (ii) is carried out by using equipment situated in the territory of a Member State (cf. Art. 4 No. 1 lit. c Data Protection Directive). The triggers for the applicability of European data protection law provided by the Data Protection Directive were therefore the establishment of a controller and the place of data processing. As provided in the Commission's proposal for the GDPR (see COM (2012) 11/4), the GDPR maintains the first trigger to a large extent (cf. Art. 3 para. 1) but replaces the second trigger (place of data processing) with the location of the data subject. Pursuant to Art. 3 para. 2, the GDPR also applies to controllers without an establishment in the EU if the data processing is related to: (a) the offering of goods or services to data subjects in the Union, irrespective of whether a payment of the data subject is required; or (b) the monitoring of their behaviour as far as their behaviour takes place within the EU (Art. 3 para. 2). These provisions are supposed to ensure that non-EU internet companies that compete with EU-companies in the European market comply with the same data protection laws. For further guidance regarding the territorial scope of the GDPR, see the EDPB's Guidelines 3/2018 on the territorial scope of the GDPR (Article 3), 12 November 2019, available at https://edpb.europa.eu/our-work-tools/our-documents/riktlinjer/guidelines-32018-territorial-scope-gdpr-article-3-version_en.

2 A processing takes place "**in the context of the activities**" of an establishment if the establishment itself performs the processing or if there is at least a close connection between the data processing and the activities of the establishment. This applies if the processing takes place for the purposes of the establishment. In its judgment *Google Spain* the CJEU decided that the processing takes place "**in the context of the activities**" of an establishment, "when the operator of a search engine [established in the US] sets up in a Member State a branch or subsidiary which is intended to promote and sell advertising space offered by that engine and which orientates its activity towards the inhabitants of that Member State" (CJEU 13 May 2014, C-131/12, para. 60). Pursuant to this broad interpretation, it might be sufficient if the activities of an establishment commercially promote the parent company's data processing. The CJEU confirmed this position (see CJEU 24 September 2019, C-507/17 – *Google LLC/*

CNIL, para. 52). According to the EDPB "the meaning of 'processing in the context of the activities of an establishment of a controller or a processor' is to be understood in light of the relevant case law" (EDPB, Guidelines 3/2018 on the territorial scope of the GDPR (Article 3), 12 November 2019, at 7, available at https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_3_2018_territorial_scope_after_public_consultation_en_1.pdf).

3 Pursuant to Recital 22, the term "**establishment**" requires "the effective and real exercise of activity through stable arrangements", where the legal form of the establishment – "whether through a branch or a subsidiary with legal personality" – is not decisive. This is the same wording used in Recital 19 of the Data Protection Directive. Therefore, the previous case law of the CJEU applies pursuant to which also subsidiaries with legal personality constitute an establishment (CJEU 13 May 2014, C-131/12 – *Google Spain*) even if the establishment with legal personality does not operate in the core business of the parent company (but merely sells advertisement, as in *Google Spain*). In its *Weltimmo* judgment dated 1 October 2015, the CJEU interpreted the term "establishment" under the Data Protection Directive broadly and stated that "the presence of only one representative can, in some circumstances, suffice to constitute a stable arrangement if that representative acts with a sufficient degree of stability through the presence of the necessary equipment for provision of the specific services concerned in the Member State in question" (CJEU 1 October 2015, C-230/14 – *Weltimmo*, para. 31). Pursuant to the CJEU, a "real and effective activity" might already apply if it is a "minimal one" (CJEU 1 October 2015, C-230/14 – *Weltimmo*, para. 31). This is true for "the running of one or several property dealing websites concerning properties situated in Hungary, which are written in Hungarian and whose advertisements are subject to a fee after a period of one month" (CJEU 1 October 2015, C-230/14 – *Weltimmo*, para. 32). The EDPB states that "[t]he threshold for 'stable arrangement' can actually be quite low" and thus, "in some circumstances, the presence of one single employee or agent of a non-EU entity in the Union may be sufficient to constitute a stable arrangement" (EDPB, Guidelines 3/2018 on the territorial scope of the GDPR (Article 3), 12 November 2019, at 6, available at https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_3_2018_territorial_scope_after_public_consultation_en_1.pdf). A website's accessibility in a Member State does not constitute an establishment (CJEU 28 July 2016, C-191/15 – *VKI v Amazon*, para. 76). This has also been confirmed by the EDPB (see EDPB, Guidelines 3/2018 on the territorial scope of the GDPR (Article 3), 12 November 2019, at 6, available at https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_3_2018_territorial_scope_after_public_consultation_en_1.pdf).

4 The **personal scope** of the GDPR is significantly extended compared to the Data Protection Directive because the GDPR not only obligates the controller but **also the processor**. The territorial scope does not only focus on the establishment of the controller, but also on the establishment of the processor. That means that the obligations of the processor pursuant to the GDPR – in particular to not engage a subprocessor without prior separate or general consent of the

controller (Art. 28 para. 2), to maintain records of each category of processing activity (Art. 30 para. 2), to appoint a data protection officer (Art. 37), and to transfer personal data to third countries only in compliance with Chapter V – also apply to a processor located in the EU, even if the processor processes personal data for a controller that is not subject to the GDPR (which again, cf. cmt. 1 above, requires that the controller neither has an establishment in the EU nor addresses the European market). This makes little practical sense because the data usually are subject to less data protection at the controller's location anyway. This will limit the competitiveness of European processors which offer their services for example in the US because competing US-based processors and the controller itself are not subject to such obligations.

5 Since the incorporation into the **EEA Agreement**, the GDPR also applies in Iceland, Liechtenstein and Norway (cf. www.efta.int/media/documents/legal-texts/eea/other-legal-documents/adopted-joint-committee-decisions/2018%20-%20English/154-2018.pdf).

6 Since para. 2 addresses controllers and processors, the GDPR may also apply to processors without an establishment in the EU that offer services to controllers in the EU (see also cmt. 8 below). The EDPB considers "that, where processing activities by a controller relates to the offering of goods or services or to the monitoring of individuals' behaviour in the Union ('targeting'), any processor instructed to carry out that processing activity on behalf of the controller will fall within the scope of the GDPR by virtue of Art 3(2) in respect of that processing" (EDPB, Guidelines 3/2018 on the territorial scope of the GDPR (Article 3), 12 November 2019, at 11, available at https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_3_2018_territorial_scope_after_public_consultation_en_1.pdf). The EDPB seems to consider the GDPR applicable for a processor that offers a service to a controller for purposes of enabling the controller to offer goods/services via the service to individuals in the EU, although it is not the processor but the controller that offers the goods/services to individuals. In our opinion, notwithstanding this, transfers to such processors must comply with the provisions regarding the transfer of personal data to third countries pursuant to Art. 44 et seq. (cf. Art. 44 cmt. 3).

7 Due to the wording in para. 2, there is the following **gap** in relation to para. 1: A controller, or a processor established outside the Union which monitors the behaviour of data subjects in the Union (or offers goods or services to data subjects in the Union, whose data it is processing) may, at least pursuant to the clear language of para. 2, avoid the applicability of the GDPR by establishing a subsidiary (or other establishment; cf. cmt. 3) in the Union, without processing data in the context of the activities of such an establishment. In such a case the wording of para. 2 does not apply because the controller, or processor, is not "established in the Union". Para. 1 does not apply either because the processing would not take place "in the context of the activities of the establishment" of the controller in the Union. However, it might be argued that para. 2 must be extended to controllers and processors that have an establishment in the Union because, in such a case, the connection to the laws of the Union are

even stronger than in the situation explicitly described in para. 2. It also has to be considered that the CJEU's requirements regarding the existence of an establishment that processes personal data in the context of its activities are very low (cf. above cmt. 3).

8 Pursuant to Recital 23 sentence 2, it is of relevance when answering the question whether a controller or processor is offering goods or services to data subjects in the Union, "**whether it is apparent that the controller or processor envisages offering services to data subjects in one or more Member States in the Union**". Recital 23 sentence 3 furthermore states that the following circumstances would not be sufficient to ascertain such intent: (i) the mere accessibility of the controller's, processor's or an intermediary's website in the EU; (ii) the mere accessibility of an email address or of other contact details; or (iii) the use of a language generally used in the third country where the controller is established. However, such intent can be derived from Recital 23 sentence 3 for the following circumstances: (i) the use of a language or currency that is generally used in one or more Member States (but not at the place of establishment of the operator) in connection with the possibility to order goods and services in such other language; or (ii) the mentioning of customers or users that are in the Union. Regarding the targeting criterion, also see EDPB's Guidelines (EDPB, Guidelines 3/2018 on the territorial scope of the GDPR (Article 3), 12 November 2019, at 13 et seqq., available at https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_3_2018_territorial_scope_after_public_consultation_en_1.pdf).

9 Recital 24 sentence 2 clarifies that in particular the tracking (ie, logging) of internet activities of data subjects – for example to generate personalised advertisement – constitutes a "**monitoring**" within the meaning of para. 2 lit. b. The use of cookies might therefore result in such monitoring if they are used for personalising content. See also the EDPB's guidelines (EDPB, Guidelines 3/2018 on the territorial scope of the GDPR (Article 3), 12 November 2019, at 20, available at https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_3_2018_territorial_scope_after_public_consultation_en_1.pdf).

10 Recital 25 mentions a Member State's diplomatic mission or consular post in a third country as an example.

The EU General Data Protection Regulation (GDPR): A Commentary Second Edition

Lukas Feiler, Nikolaus Forgó and Michaela Nebel

Since 25 May 2018 the General Data Protection Regulation 2016/679 (GDPR) has applied, representing a significant overhaul of data protection law in the European Union. Although it was drafted and passed by the European Union, the GDPR imposes obligations onto organisations anywhere, so long as they collect or target data relating to people in the EU. It is one of the toughest privacy and security laws in the world and harsh fines are levied against those who violate its privacy and security standards.

This commentary provides a detailed examination of the individual articles of the GDPR and is an essential resource aimed at helping legal practitioners to ensure compliance. Coverage in this revised and updated second edition includes:

- a general introduction to data protection law;
- full text of the GDPR's articles and recitals; and
- article-by-article commentary explaining the individual provisions and elements of each article.

The second edition also includes guidelines on the interpretation of the GDPR published by the European Data Protection Board as well as new case law by the Court of Justice of the European Union.

In addition to lawyers and in-house counsel, this book is also suitable for law professors and students, and offers comprehensive coverage of this important area of data protection legislation.

Globe Law and Business

GLP
German Law Publishers

ISBN 978-1-787424-78-4