# THE EU GENERAL DATA PROTECTION REGULATION: A NEW GLOBAL STANDARD FOR INFORMATION PRIVACY

Bart van der Sloot & Frederik Zuiderveen Borgesius[1]

B.vdrsloot [at ] uvt.nl & Frederik.Zuiderveen.Borgesius [at] vub.ac.be

*- Working draft. Please contact us before citing.*

*We'd love to hear your comments Thanks! -*

**Abstract** - This paper discusses the General Data Protection Regulation (GDPR) of the European Union, which enters into force in May 2018. The Regulation will replace the 1995 Data Protection Directive, one of the world's most influential data privacy laws. This paper describes and analyzes the GDPR. Data protection law's core principles, also known as the Fair Information Principles, are retained in the GDPR. However, the GDPR also brings significant changes. For instance, unlike a directive, a regulation does not have to be implemented in the national laws of the EU Member States. Hence, the GDPR should lead to a more harmonized regime in Europe. Furthermore, the enforcement mechanisms are strengthened. Data Protection Authorities can impose fines for non-compliance of up to 4% of the worldwide turnover of companies. This also applies to, for instance, American companies operating in Europe or gathering data about people in Europe. Hence, the GDPR, the world's strictest and most comprehensive data privacy law, will influence policy worldwide.

[1] As in our earlier publications, both authors contributed equally to the paper.

**Table of Contents**

# 1. INTRODUCTION

This paper discusses the General Data Protection Regulation ("GDPR") of the European Union,[2] which was adopted in 2016, and will enter into force in 2018.[3] It shows the most important changes the GDPR will bring[4] in comparison to the 1995 Data Protection Directive ("Directive").[5] The paper aims to discuss the GDPR in such a way that readers who are not specialized in European law or in data protection law can follow the text.

The paper is structured as follows. Section 2 provides the historical background and political context of European data protection law and the GDPR. Section 3 discusses the GDPR's material and territorial scope – the conditions for its applicability. Section 4 introduces the GDPR, its core principles, and the requirements for legitimate processing activities. Section 5 turns to the responsibilities of data controllers and data processors, that is, the companies and parties that process data about others. Section 6 discusses the rights of the data subject, such as the right to be forgotten and the right to object to profiling. Section 7 discusses enforcement of the GDPR, through sanctions, fines, and increased cooperation between regulatory bodies. Section 8 offers concluding thoughts: the GDPR is the world's strictest and most comprehensive data privacy law and will influence policy worldwide.

# 2. BACKGROUND TO THE GDPR

Privacy is recognized as a human right in Europe.6 For instance, Article 8 of the 1950 European Convention on Human Rights provides protection to private and family life, home, and communication.[7] This provision is inspired by the right to privacy as protected by the 1948 United Nations Declaration of Human Rights[8] and is similar to

---

[2] Regulation (EU) 2016/679 Of the European Parliament and of the Council Of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf

[3] Article 99(2) GDPR: "It shall apply from 25 May 2018."

[4] See also: Article 29 Working Party, 'Statement on the 2016 action plan for the implementation of the General Data Protection Regulation (GDPR)', 442/16/EN, WP 236, 2 February 2016.

[5] The EU also adopted a new directive regarding personal data processing in the police sector, which replaces an older Council Framework Decision. An analysis of that directive, however, falls outside this paper's scope. Directive (EU) 2016/680 of the European Parliament and of The Council of 27 April 2016 on 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, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA. See on that directive: P. De Hert and V. Papakonstantinou Vagelis, *The New Police And Criminal Justice Data Protection Directive. A First Analysis*, New Journal of European Criminal Law (1) 7(1): 7-19.

[6] In this paper, we use the phrases "human right" and "fundamental right" interchangeably. See on the difference: G. Gonzalez Fuster, The Emergence of Personal Data Protection as a Fundamental Right, Springer, 2014, p. 164-166.

[7] Convention for the Protection of Human Rights and Fundamental Freedoms, Article 8, 4 November 1950, 213 U.N.T.S. 222.

[8] Universal Declaration of Human Rights, Article 12, G.A. Res. 217A (III), U.N. Doc. A/810 at 71 (1948).

the 1966 International Covenant on Civil and Political Rights.[9] Most national constitutions in Europe also protect privacy and related rights, such as the right to the inviolability of the body, the sanctity of the home, the secrecy of communication, and the protection of one's personality.[10]

Data protection law in Europe covers topics that are often discussed under the heading "data privacy" or "information privacy" in the US.[11] In Europe, however, the right to data protection is increasingly seen as separate from the right to privacy. Data protection law is not so much concerned with protecting people's private affairs; rather it generally aims to ensure fairness and procedural diligence when personal data are processed.[12]

In Europe, two international organizations have been particularly important for data protection law: the Council of Europe and the European Union.[13] The Council of Europe took some of the earliest steps in the field of data protection law. In 1950, it adopted the European Convention on Human Rights, which contains the right to privacy. The European Court of Human Rights, overseeing the Convention, has interpreted that provision broadly, so the provision also provides protection when personal data are processed.[14] In addition, the Council of Europe adopted two resolutions, in 1973 and 1974, with principles for the protection of privacy in the area of digital data processing for the private and the public sectors.[15] In 1981, the Council of Europe adopted the first legally binding international instrument on data protection, the Data Protection Convention.[16] This instrument is still in place and requires signatories to enact data protection provisions in their national laws.[17]

---

[9] International Covenant on Civil and Political Rights Article 17, 16 December 1966, S. Treaty Doc. No. 95-20, 6 I.L.M. 368 (1967), 999 U.N.T.S. 171.

[10] See for example Article 2 of the German Constitution. See on constitutional protection of privacy in other countries: B.J. Koops, B. Newell, Bryce, T. Timan, I. Škorvánek, T. Chokrevski, M. Galič, *A Typology of Privacy*, University of Pennsylvania Journal of International Law 38(2): 483-575 (2017).

[11] Information privacy "concerns the collection, use and disclosure of personal information", P. M. Schwartz & D. J. Solove, Information Privacy, Aspen 2009, p. 1. Data privacy and information privacy refer to roughly the same concept.

[12] G. Gonzalez Fuster, The Emergence of Personal Data Protection as a Fundamental Right, Springer, 2014

[13] See also C. J. Bennett, *Regulating Privacy: Data Protection and Public Policy in Europe and the United States*, Cornell University Press 1992.

[14] See: P. Hert P and S. Gutwirth, 'Data protection in the Case Law of Strasbourg and Luxemburg: constitutionalisation in action' in Gutwirth, S. and others (eds), *Reinventing data protection?* (Springer 2009).

[15] Council of Europe, Committee of Ministers, Resolution (73)22 on the protection of the privacy of individuals *vis-à-vis* electronic data banks in the private sector, 26 September 1973; Committee of Ministers, Resolution (74)29 on the protection of the privacy of individuals *vis-à-vis* electronic data banks in the public sector, 20 September 1974.

[16] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data CETS No.: 108, 28 January 1981.

[17] Article 4(1) of the Data Protection Convention 1981. The Data Protection Convention is being revised: http://www.coe.int/en/web/data-protection/modernisation-convention108.

The Council of Europe counts 47 countries as its members; only a handful of European countries, such as the Vatican City and Belarus, are not part of the Council.[18] The Council of Europe was founded just after the Second World War, and is focused mainly on the protection of human rights and peaceful cooperation between the European countries.

By contrast, the European Union has 28 member countries; 27 when the United Kingdom leaves the EU. The European Union was originally primarily focused on economic cooperation, but has gradually also focused on human rights protection. The EU has adopted a Charter of Fundamental Rights of the European Union in 2009. The Charter, like the European Convention on Human Rights from 1950, contains the right to privacy, but in addition, includes a separate fundamental right to data protection.

> Article 7 - Respect for private and family life
>
> Everyone has the right to respect for his or her private and family life, home and communications.
>
> Article 8 - Protection of personal data
>
> 1. Everyone has the right to the protection of personal data concerning him or her.
> 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
> 3. Compliance with these rules shall be subject to control by an independent authority.[19]

In 1990, the European Commission feared that diverging national data protection laws would hinder the internal market.[20] That year, it published a proposal for a Data Protection Directive. After five years of negotiations, the final Data Protection Directive was adopted in 1995.[21] The Directive laid down an omnibus regime, which applied to most of the private and public sector (with exceptions to the latter).[22] The

---

[18] http://www.coe.int/en/web/portal/47-members-states

[19] Charter of Fundamental Rights of the European Union, http://www.europarl.europa.eu/charter/pdf/text_en.pdf. The Charter was adopted in 2000, and was made a legally binding instrument by the Lisbon Treaty of 2009.

[20] The European Commission proposes and enforces legislation and implements policies and the EU budget. https://ec.europa.eu/commission/index_en

[21] A. Newman, Protectors of privacy: regulating personal data in the global economy (Cornell University Press 2008).

[22] Some parts of the public sector are outside the scope of the Directive (see Article 3(2) and Article 13). Some data processing practices in the private sector are partially exempted; processing for purely personal purposes (Article 3(2)), and for journalistic purposes (Article 9).

Data Protection Directive has influenced the law in many countries outside the EU.[23] Around 120 countries have laws that are based on the same principles as the Directive.[24]

One of the main problems with the Directive is the compliance and enforcement deficit. Many companies and organizations do not comply with the Directive, and enforcement leaves something to be desired. Hence, within the EU a large gap currently exists between law and practice. This was the most important reason for the EU lawmaker proposing a new data protection instrument to replace the Directive. Although, by and large, the material provisions, rights, and obligations have remained the same, the essential objective of the GDPR is to close the gap between law and practice.

Following a consultation period that started in 2009,[25] the European Commission published a proposal for a General Data Protection Regulation in early 2012.[26] In 2014, the European Parliament adopted a compromise text, based on the 3,999 amendments proposed by the members of parliament.[27] The Council of the European Union published its proposal for the GDPR in 2015, to start negotiations with the European Parliament.[28] In December 2015, the Parliament and Council reached agreement on the text of the GDPR. More than four years after the first proposal, the GDPR was officially adopted in May 2016.

In the GDPR's preamble, the EU lawmaker notes that more and more personal data are being collected and used,[29] and that people "increasingly make personal information available publicly and globally."[30] With the GDPR, the EU lawmaker aims for a "strong

---

[23] M. Birnhack, *The EU Data Protection Directive: An Engine of a Global Regime*, Computer Law & Security Review, 2008, 24(6) 508. M. Birnhack, *Reverse Engineering Informational Privacy Law,* 15 Yale Journal of Law & Technology, 24, 2012; A. Bradford, *The Brussels effect* (2012) 107 Nw.UL Rev. 1.

[24] In January 2017, Greenleaf counted 120 countries in the world with a data protection law. Greenleaf, *Global Data Privacy Laws 2017: 120 National Data Privacy Laws, Including Indonesia and Turkey* (January 30, 2017), 145 Privacy Laws & Business International Report, 10-13; UNSW Law Research Paper No. 45, https://ssrn.com/abstract=2993035.

[25] European Commission, Commission Staff Working Paper, Impact Assessment Accompanying the document Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) and Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data {COM(2012) 10 final} {COM(2012) 11 final} {SEC(2012) 73 final}, Brussels, 25 January 2012 SEC(2012) 72 final, p. 8.

[26] The European Parliament is a EU body with legislative, supervisory, and budgetary responsibilities. It is directly elected. http://www.europarl.europa.eu/portal/

[27] LIBE Compromise, proposal for a Data Protection Regulation (this paper refers to the unofficial Consolidated Version after LIBE Committee Vote, provided by the Rapporteur, General Data Protection Regulation, 22 October 2013 <www.janalbrecht.eu/fileadmin/material/Dokumente/DPR-Regulation-inofficial-consolidated-LIBE.pdf> accessed 24 January 2016).

[28] The Council of the European Union consists of government ministers from each EU country, according to the policy area to be discussed. http://www.consilium.europa.eu/en/home/.

[29] Recital 5 GDPR: "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."

[30] Recital 6 GDPR.

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."[31] The EU lawmaker aims for more legal certainty, strengthened enforcement, and better harmonization.[32]

A directive, such as the 1995 Data Protection Directive, is binding as to the result to be achieved, but leaves the choice of form and methods to the Member States. Member States must implement a directive in their national legal systems; usually they do this through a national act.[33] This therefore resulted in significant differences in the data protection rules adopted at Member State level, which allowed for forum shopping. Data companies sometimes decided to place their headquarters in the country with the lowest regulatory pressure, in order to avoid some or all of the obligations under the Data Protection Directive. Some speak of data protection law's "loophole" in Ireland.[34] This will change. Unlike a directive, a regulation does not have to be implemented in the national laws of the EU Member States.[35] Hence, the GDPR should lead to a more harmonized regime in Europe. Also, less divergence between national rules should make it easier for companies to do cross-border business.[36]

The Court of Justice of the European Union is the highest authority on the interpretation of EU law.[37] In addition, there are the opinions of the Article 29 Working Party, an advisory body in which the national Data Protection Authorities of the European Union cooperate.[38] The Working Party publishes opinions on all matters relating to personal data processing,[39] and has published more than 200 opinions. The opinions of the Working Party are not legally binding, but they are influential.[40] Where relevant, this paper refers to case law of the Court of Justice of the European Union and to opinions of the Working Party. The paper also refers to recitals. EU legal texts start with a

---

[31] Recital 7 GDPR.
[32] Recital 7 GDPR.
[33] Article 288 of the Treaty on the Functioning of the European Union http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012E/TXT&from=EN.
[34] Albrecht, *#EUdataP State of the Union*, speech at the Chaos Communication Congress, 2013, http://www.janalbrecht.eu/fileadmin/material/Dokumente/30C3-JPA-EUdataP.pdf.
[35] Article 288 of the Treaty on the Functioning of the European Union http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012E/TXT&from=EN.
[36] However, differences may remain between the Member States. C. Burton et al., *The Final European Union General Data Protection Regulation*, <https://www.wsgr.com/publications/pdfsearch/bloombergbna-0116.pdf>, p. 13.
[37] National judges in the EU can, and in some cases must, ask the Court of Justice of the European Union if they are unsure how to interpret EU rules. For instance, if a national judge does not know how to interpret a national provision that is based on an EU directive, the national judge must ask advice from the Court of Justice of the European Union.
[38] Article 29(2) Data Protection Directive.
[39] Articles 29 and 30 Data Protection Directive.
[40] Although the Working Party can adopt opinions after a vote, it usually takes decisions by consensus. See generally on the Working Party: Yves Poullet & Serge Gutwirth, *The Contribution of the Article 29 Working Party to the Construction of a Harmonised European Data Protection System: An Illustration of "Reflexive Governance"?*, in M. V. Perez Asinari & P. Palazzi (eds), Défis Du Droit A La Protection De La Vie Privée, Bruylant, 2008.

preamble, comprising recitals. These recitals can be used to interpret material provisions in directives and regulations.[41]

Like the Directive from 1995, the GDPR's first article stresses that the GDPR has a dual goal.[42] First, the GDPR "protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data."[43] Second, the GDPR states that "[t]he 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."[44] Hence, the GDPR has a dual aim.[45]

## 3. THE APPLICABILITY OF THE GDPR

For the GDPR to apply, certain conditions must be fulfilled. These are discussed below. First, "personal data" should be "processed". Second, it should be determined who is responsible for complying with the GDPR. Third, the GDPR should be applicable in terms of territorial scope. Fourth, exceptions may exclude the application of the GDPR in whole or in part.

### *3.1 When are "personal data" being "processed"?*

The GDPR applies when "personal data" are "processed" (subject to exceptions). Almost everything that can be done with personal data, such as storing, analyzing, selling, and even deleting personal data, falls within the definition of "processing".[46] "Personal data" are defined as follows:

> "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,

---

[41] Courts sometimes refer to recitals in data protection cases. See e.g. CJEU, Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González, C-131/12, 13 May 2014. See generally on the role of recitals: T. Klimas & J. Vaičiukaitė, *The Law of Recitals in European Community Legislation* ILSA Journal of International & Comparative Law, 15, 2008, p. 3. "Where the recital is clear, it will control an ambiguous operative provision. This means that the operative provision will be interpreted in the light of the recital".

[42] Article 1(1) GDPR. The GDPR "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."

[43] Article 1(2) GDPR.

[44] Article 1(3) GDPR.

[45] Other international data protection texts also have the dual goal of aiming for fair data processing and the free movement of personal data over borders. See e.g. the Council of Europe Data Protection Convention and the OECD Data Protection Guidelines.

[46] Article 4(2) GDPR.

> physiological, genetic, mental, economic, cultural or social identity of that natural person.[47]

The GDPR applies to personal data of "natural persons, whatever their nationality or place of residence, in relation to the processing of their personal data."[48] A natural person is, in short, not a legal person,[49] and not a deceased person.[50] The person whose data are being processed is called the data subject.

The concept of personal data is much broader than personally identifiable information such as names or addresses.[51] In brief, every datum that identifies a person or could identity a person in the future is a piece of personal data.[52] Public and non-sensitive information can also fall within the scope of "personal data". The Article 29 Working Party provides: "Even ancillary information, such as "the man wearing a black suit" may identify someone out of the passers-by standing at a traffic light."[53] In addition, data are not only considered "personal" when they can be used to identify a person, but also when that person can be "individualized", meaning that he or she can be singled out and be treated in a specific manner, without knowing the person's exact identity.[54]

The phrase "identifiable" (person) in the Directive's personal data definition has led to discussion. Someone is "identifiable" if he or she "can be identified, directly or indirectly."[55] The Court of Justice has decided that IP addresses generally constitute personal data.[56] The GDPR's preamble emphasizes that tracking cookies and similar identifiers can be used to identify people:

---

[47] Article 4(1) GDPR; capitalization and interpunction adapted.
[48] Recital 14 GDPR.
[49] Recital 14 GDPR. See about the protection of legal persons also LA Bygrave, *Data protection law: approaching its rationale, logic and limits (PhD thesis University of Oslo)*, vol 10 (Information Law Series, Kluwer Law International 2002); B. Van der Sloot, *Do Privacy and Data Protection Rules Apply to Legal Persons and should they? A Proposal for a Two-Tiered System,* 31 Computer Law & Security Review 26 (2015).
[50] Recital 27 GDPR. See the special on post mortem privacy on SCRIPT-ed: https://script-ed.org/archive/volume-10/issue-101-1-139/
[51] See Article 29 Working Party, 'Opinion 4/2007 on the concept of personal data' (WP 136), 20 June 2007; Schwartz PM and Solove DJ, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information* (2011) 86 New York University Law Review 1814.
[52] Anonymous data fall outside the scope of the GDPR. See also: Article 29 Working Party, 'Opinion 05/2014 on Anonymisation Techniques' (WP216), 10 April 2015.
[53] Article 29 Working Party, 'Opinion 4/2007 on the concept of personal data' (WP 136), 20 June 2007, p.13.
[54] Frederik J. Zuiderveen Borgesius, *Singling Out People without Knowing their names–Behavioural Targeting, Pseudonymous Data, and the New Data Protection Regulation,* 32 Computer Law & Security Review 256 (2016); Article 29 Working Party, 'Opinion 4/2007 on the concept of personal data' (WP 136), 20 June 2007
[55] Article 4(1) GDPR.
[56] Case CJEU, Patrick Breyer v Bundesrepublik Deutschland, Case C-582/14, 19 October 2016. See also: CJEU, Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM), intervening parties: Belgian Entertainment Association Video ASBL (BEA Video), Belgian Entertainment Association Music ASBL (BEA Music), Internet Service Provider Association ASBL (ISPA), Case C-70/10, 24 November 2011.

> 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.57

Because of its wide scope, almost every governmental organization, company, and even individual "processes" "personal data", and thus potentially falls under the EU data protection regime. Therefore, the definition of personal data has led to much lobbying during the negotiations on the GDPR. Many companies argued that pseudonymous data, nameless data that refer to individuals, should remain outside the scope of the rules, or should be governed by a lighter regime.[58] On this point, the lobbying was not successful. The GDPR's preamble says that pseudonymous data can still be personal data.[59] Still, the GDPR recommends pseudonymization as a security measure.[60]

Consequently, whenever a party processes data that relate to a natural person, whether the data is public or private, sensitive or non-sensitive, directly or indirectly identifies that person, and whether identification is possible now or in the future, it processes "personal data" within the meaning of the GDPR. The GDPR has even broadened the scope of the term "personal data" by adding "location data" and "online identifiers" as examples of identifiers in the GDPR's personal data definition.[61]

### *3.2 Who is accountable for upholding the GDPR requirements?*

When it is clear that personal data are being processed, the question is who is responsible for upholding the rules and obligations under the EU data protection framework. The GDPR distinguishes between a number of parties, with different responsibilities. Besides the data subject (the person that can be identified through the personal data), the most important party is the data controller. The data controller is the natural or legal person who, alone or jointly with others, determines on the one hand the purposes and on the other hand the means of the processing of personal data.[62] The controller is primarily responsible for upholding the data protection principles.

---

[57] Recital 30 GDPR. See also Recitals 26-29.
[58] Frederik J. Zuiderveen Borgesius, *Singling Out People without Knowing their names–Behavioural Targeting, Pseudonymous Data, and the New Data Protection Regulation,* 32 Computer Law & Security Review 256 (2016).
[59] Recital 26 GDPR: "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."
[60] Article 4(5) GDPR. See also Recitals 28 and 29 GDPR.
[61] See in detail on the personal data definition: F.J. Zuiderveen Borgesius, *Singling out people without knowing their names–Behavioural targeting, pseudonymous data, and the new Data Protection Regulation'*, Computer Law & Security Review 32.2 (2016): 256-271.
[62] Article 4(7) GDPR.

There are many instances in which there is more than one data controller and increasingly situations in which it is mostly unclear who is really responsible for the processing of data; a prominent example is websites that work with user-generated content. If a user of Facebook, YouTube, or news sites that host user-generated content posts personal data about another person, without, for example, having a legitimate basis for it, the question is who is responsible for the violation of the data protection rules, the user or the platform. While the user provides the content, the businesses provide the platform and the technical means for processing the data.[63]

It can be argued that in fact, both parties are jointly responsible for the upholding of the legal principles, pointing to the fact that the definition of "data controller" refers to the person who "alone or jointly" is responsible for the processing of the data. As the definition of "data controller" has remained largely the same in the GDPR as in the Data Protection Directive, no clarity is brought on this point.

The position of "processor" was often unclear under the Directive, while in practice, this position is becoming increasingly important.[64] The processor is the party that processes data on behalf of the data controller.[65] For example, if company Y gathers and analyzes survey data on the customers of company X, as instructed by company X, company Y will typically be the data processor.[66]

What is clear, however, is that many of the obligations that under the Directive only applied to the data controller will under the GDPR also apply to data processors. This will be explained in more detail later on – in short, even parties processing on behalf of a data controller, such as a data center or cloud provider, have to comply with a considerable proportion of the GDPR when they process personal data of EU citizens, even when the databases or companies are based in the US.[67]

### *3.3 When does the GDPR apply to non-EU companies?*

It is clear that natural and legal persons that process personal data will fall under the GDPR if they are based in the EU. But the same may hold true if they are based in a non-EU country such as the US.[68] The GDPR intends to provide protection to all natural

---

[63] See on the interplay between platforms and data protection law: D. Erdos, *Delimiting the Ambit of Responsibility of Intermediary Publishers for Third Party Rights in European Data Protection: Towards a Synthetic Interpretation of the EU acquis* (June 27, 2017). University of Cambridge Faculty of Law Research Paper No. 31/2017. https://ssrn.com/abstract=2993154

[64] See on sub-processors: Article 29 Working Party, 'Working document 01/2014 on Draft Ad hoc contractual clauses "EU data processor to non-EU sub-processor"', 757/14/EN, WP 214, 21 March 2014.

[65] Article 4(7) GDPR.

[66] See further: Article 29 Working Party, 'Opinion 1/2010 on the concepts of "controller" and "processor"', 00264/10/EN, WP 169, 16 February 2010. See also chapter 5 of this paper.

[67] There are several other positions, such as the recipient, the third party and the representative, but these positions fall outside the scope of this paper.

[68] See: Article 29 Working Party, 'Update of Opinion 8/2010 on applicable law in light of the CJEU judgement in Google Spain' (WP179 update), Brussels, 16 December 2015.

persons, whatever their nationality or residence.[69] But for the GDPR to apply, there must be a link with the EU. There are four instances in which the GDPR will apply.[70]

The main rule is that the GDPR will apply when personal data are being processed "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."[71] The Court of Justice has decided that Google Spain is an establishment of Google Inc., and that some of the advertising activities aimed at the Spanish public were "carried out in the context of the activities" of the Spanish establishment, so Google had to comply with EU law.[72] In this case, Google Spain is the relevant establishment.

Second, the GDPR can apply to data controllers or data processors not established in the EU when a natural or legal person offers goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union.[73] This situation could apply, for instance, if a US company offers an online email service to data subjects in the EU, and processes personal data of those data subjects.[74] This rule applies when it is "apparent that the controller or processor envisages offering services to data subjects in one or more Member States in the Union."[75] The mere fact that a website is accessible from the EU is insufficient. When assessing whether a service is offered to people in the EU, relevant factors are, for instance, whether a website uses a language or currency used in the EU.[76]

Third, the GDPR can apply to data controllers or data processors not established in the EU when a natural or legal person uses personal data for monitoring the behavior of EU citizens, as far as their behavior takes place within the Union.[77] This rule applies, inter alia, if a behavioral targeting company tracks the browsing behavior of a data subject in the EU. Hence, many marketing companies that are established outside the EU may fall within the territorial scope of the GDPR if they track the online behavior of people in the EU. It appears from the GDPR's preamble that the rule is written specifically for online tracking.[78]

Finally, the GDPR applies where Member State law applies by virtue of public international law, to a controller not established in the Union, such as in a Member State's diplomatic mission or consular post.[79] This provision refers to embassies and similar organizations.

---

[69] Recital 2 GDPR.
[70] See for the situation under the Directive, among others: CJEU, Verein für Konsumenteninformation v Amazon EU Sàrl, C-191/15, 28 July 2016.
[71] Article 3(1) GDPR.
[72] Case C-131/12, Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos and Mario Costeja González. See also: Article 29 Working Party, 'Update of Opinion 8/2010 on applicable law in light of the CJEU judgement in Google Spain' (WP179 update), Brussels 16 December 2015.
[73] Article 3(2)(a) GDPR.
[74] See Recitals 22-24 GDPR.
[75] Recital 23 GDPR.
[76] Recital 23 GDPR.
[77] Article 3(2) GDPR.
[78] Recital 24 GDPR.
[79] Article 3(3) GDPR.

In sum, the term "processing" is wide, as is the notion of "personal data". In addition, many different parties involved in the data process have obligations under the GDPR. Finally, the territorial scope of the GDPR means that many international firms processing data of people in Europe will need to respect the EU data protection framework.

### *3.4 What are the exceptions from the application of the GDPR?*

Certain processing activities fall outside the GDPR's scope. Four situations are of special importance.[80] First, there is an exemption for a "purely personal or household activity". The Court of Justice of the European Union has decided that when the surroundings of a house are filmed by a video camera attached to the home, for the purpose of identifying burglars, this will not count as a "purely personal or household activity".[81] The GDPR's preamble shows that "correspondence and the holding of addresses, or social networking" is an example of a situation that falls under the household exception.[82] For example, if somebody sends a letter to a friend in which he writes about his nephew, this will normally not fall under the GDPR.

Second, also outside the GDPR's reach are processing activities concerning national security.[83] The EU and Member States are also allowed to restrict some of the GDPR's rules when this is necessary and proportionate in relation to the protection of national security,[84] the prevention and prosecution of criminal offences,[85] or the protection of the data subject or the rights and freedoms of others.[86] The EU adopted a separate directive in 2016 for personal data processing by the police and similar bodies, a discussion of which falls outside the scope of this paper.[87]

Third, there is a special regime for freedom of expression.[88] The Directive contained a special provision on the processing of personal data in the context of freedom of speech.

---

[80] There are also special rules for national identification numbers (Article 87 GDPR), the context of employment (Article 88 GDPR), obligations of professional secrecy (Article 90 GDPR), and religious associations (Article 91 GDPR).

[81] CJEU, František Ryneš v. Úřad pro ochranu osobních údajů, C-212/13, 11 December 2014.

[82] Recital 18 GDPR.

[83] Recital 16 GDPR. See A. Arnbak, Securing Private Communications, Kluwer Law International 2016.

[84] See also: CJEU, Institut professionnel des agents immobiliers (IPI) v Geoffrey Englebert, Immo 9 SPRL, Grégory Francotte, intervening parties: Union professionnelle nationale des détectives privés de Belgique (UPNDP), Association professionnelle des inspecteurs et experts d'assurances ASBL (APIEA), Conseil des ministres, Case C-473/12, 7 November 2013.

[85] See also: Article 29 Working Party, 'Guidelines for Member States on the criteria to ensure compliance with data protection requirements in the context of the automatic exchange of personal data for tax purposes', 175/16/EN, WP 234, 16 December 2015.

[86] Article 23 GDPR; Recital 73 GDPR.

[87] Recital 19 GDPR. Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (OJ L 241, 17.9.2015, p. 1).

[88] See further: ECJ, Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy, Satamedia Oy, Case C-73/07, 16 December 2008. See also: D. Erdos, *European Regulatory Interpretation of the Interface between Data Protection and Journalistic Freedom: An Incomplete and Imperfect Balancing Act?,* University of Cambridge Faculty of Law Research Paper No. 61/2015. https://ssrn.com/abstract=2683471

The provision allowed Member States to make exceptions to certain provisions in the Directive for personal data processing carried out solely for journalistic purposes or the purpose of artistic or literary expression, only if the exceptions are necessary to reconcile the right to privacy with freedom of expression.[89] There was considerable discussion about this exception during the drafting process for the GDPR. In the end, however, the provision that made it into the final text is quite similar to that of the Directive. The provision stresses that Member States should adequately balance the data protection and freedom of speech interests and that some of the data protection rules do not apply when personal data are processed for journalistic purposes.[90] Hence, the GDPR will provide little harmonization regarding the balance between freedom of information and data protection. Perhaps case law of the Court of Justice of the European Union will provide more guidance.[91]

Finally, there is a special regime for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes. Like the regime for the relationship between data protection and freedom of expression, the GDPR allows some derogation of a small number of provisions, but leaves most intact. The Directive already contained a number of rules on the processing of data for statistical analysis and scientific research. The GDPR specifies that 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 a number of provisions of the GDPR.[92] In addition, there are special rules for public access to official public sector documents containing personal data.[93]

## 4. THE LEGITIMACY OF DATA PROCESSING UNDER THE GDPR

When the GDPR applies to a data processing initiative, the data controller must ensure that the process accords with the GDPR's minimum standards of legitimacy. This means, first, adhering to the fair information principles carved out according to European standards. Second, the controller must have a legitimate ground for processing personal data. Third, if the controller processes "special categories of personal data" (sometimes called sensitive data), it must have a legitimate ground for that too. Finally, if there is transfer of data from the EU to another territory, there must be an applicable ground that could legitimate this transfer. The GDPR meticulously sets outs which grounds can be invoked in each of those contexts.

---

[89] Article 9 Data Protection Directive.
[90] Article 85 GDPR.
[91] See for instance: CJEU, Case C-398/15 Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v Salvatore Manni, 9 March 2017.
[92] Article 89 GDPR. Recital 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."
[93] Article 86 GDPR.

The European Court of Justice has held that the principles of data quality and the obligation to have a legitimate ground for processing have direct effect, in that they may be relied on by an individual before the national courts to oust the application of rules of national law which are contrary to those provisions.[94]

### *4.1 The basic principles*

The core of the GDPR can be found in Article 5, which lists the "principles relating to processing of personal data", giving the main data protection requirements in broad terms.[95] Because the principles "remain sound", the EU lawmaker has kept them largely the same as in the Directive.[96] The GDPR thus includes the traditional principles for the fair use of personal data.[97] These European data protection principles resemble the US Fair Information Principles (FIPs).[98] Similar principles are included, for instance, in the OECD Privacy Guidelines, and the Data Protection Convention of the Council of Europe.[99] There are seven core principles that data controllers and processors must take into account in order to be compliant with the GDPR. They apply cumulatively – each of them must be fulfilled in order for the data processing to be deemed legitimate.

(1) The lawfulness, fairness, and transparency principle provides data protection law's overarching norm: personal data must be "processed lawfully, fairly and in a transparent manner in relation to the data subject."[100] The lawfulness requirement is reasonably clear: personal data processing must happen in accordance with the GDPR and other laws. The fairness requirement is less clear.[101] The fairness requirement could be compared with the general good faith requirement in some legal systems.[102]

---

[94] CJEU, Rechnungshof (C-465/00) v Österreichischer Rundfunk, Wirtschaftskammer Steiermark, Marktgemeinde Kaltenleutgeben, Land Niederösterreich, Österreichische Nationalbank, Stadt Wiener Neustadt, Austrian Airlines, Österreichische Luftverkehrs-AG, and between Christa Neukomm (C-138/01), Joseph Lauermann (C-13 9/01) and Österreichischer Rundfunk, 20 May 2003, Joined Cases C-465/00, C-138/01 and C-139/01. See also: CJEU (Third Chamber), Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) (C-468/10), Federación de Comercio Electrónico y Marketing Directo (FECEMD) (C-469/10) v Administración del Estado, intervening parties: Unión General de Trabajadores (UGT) (C-468/10 and C-469/10), Telefónica de España SAU (C-468/10), France Telecom España SA (C-468/10 and C-469/10), Telefónica Móviles de España SAU (C-469/10), Vodafone España SA (C-469/10), Asociación de Usuarios de la Comunicación (C-469/10), 24 November 2011, Joined Cases C-468/10 and C-469/10.

[95] Article 5 GDPR is based on Article 6 Data Protection Directive.

[96] Recital 9 GDPR.

[97] See generally on the data protection principles: L. A. Bygrave, Data Privacy Law: an international perspective, Oxford University Press, 2014.

[98] The FIPs can be recognized, for example, in U.S. Department of Health, Education & Warfare, Records and the Rights of Citizens, <www.justice.gov/opcl/docs/rec-com-rights.pdf>, in the US Privacy Act of 1974, Pub. L. No. 93–579, 88 Stat. 1896 (codified at 5 U.S.C. § 552a (2012)).

[99] OECD, OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, <http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm>

[100] Article 5(1)(a) GDPR.

[101] See also Recitals 39, 42, 57, 58, 60, 61, 62, 71 GDPR. The EU Charter also says that personal data processing must happen "fairly" (Article 8(2) EU Charter).

[102] See the good faith principle in the Draft Common Frame of Reference: "[t]he expression 'good faith and fair dealing' refers to a standard of conduct characterised by honesty, openness and consideration

(2) It follows from the purpose limitation principle that personal data should only be collected for a purpose that is specified in advance, and that those data should not be used for incompatible purposes. The principle is also included in the Charter of Fundamental Rights of the European Union.[103] The GDPR puts it as follows: personal data shall be "collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes."[104] The purpose limitation principle does not prohibit all secondary usage of personal data. Personal data may be processed for another purpose, if that new purpose is "not incompatible" with the original purpose. The GDPR gives, and this is new, guidance to assess whether a new purpose is compatible.[105] In brief, to assess whether a new purpose is compatible with the original purpose, the controller should consider, for instance, the link between the original and new purposes, the context in which the personal data were collected, the reasonable expectations of data subjects based on their relationship with the controller, the nature of the personal data, the consequences of the intended further processing for data subjects, and the existence of appropriate safeguards.[106]

(3) The data minimization principle says that personal data should be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed."[107] The preamble adds that "[p]ersonal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means."[108] The data minimization principle thus prohibits collecting as much personal data as possible because the data could be useful in the future. Hence, this principle conflicts with the strategy suggested by some "big data" enthusiasts.

(4) The accuracy principle requires that personal data are "accurate and, where necessary, kept up to date."[109] Data controllers must take "every reasonable step (…) to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay."[110] The accuracy principle does not always require full accuracy; it requires accuracy "having regard to the purposes" for which personal data are processed.[111] The level of accuracy required depends on the circumstances. Sometimes, inaccurate data cause considerable trouble. For instance, an inaccuracy in a credit report can cause many problems. Somebody could be denied a mortgage loan based on errors in a credit report. Data controllers

---

for the interests of the other party to the transaction or relationship in question." C. Von Bar, E. Clive & H. Chulte-Nölke, Principles, Definitions and Model Rules of European Private Law: Draft Common Frame of Reference <http://ec.europa.eu/justice/policies/civil/docs/dcfr_outline_edition_en.pdf>.

[103] Article 8(2) of the EU Charter. A similar principle is included, for instance, in the OECD Privacy Guidelines, called the "Purpose Specification Principle." See also: Article 29 Working Party, 'Opinion 03/2013 on purpose limitation', 00569/13/EN, WP 203, 2 April 2013.

[104] Article 5(1)(b) GDPR.

[105] Under certain conditions, further processing for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes is not considered to be incompatible with the initial purposes. Article 5(1)(b) GDPR.

[106] Article 6(4) GDPR; Recital 50 GDPR.

[107] Article 5(1)(c) GDPR. The data minimization principle is not explicitly included in the OECD Privacy Guidelines (but see the Collection Limitation Principle).

[108] Recital 39 GDPR.

[109] Article 5(1)(d) GDPR. See similarly: the Data Quality Principle of the OECD Privacy Guidelines.

[110] Article 5(1)(d) GDPR. See also Recital 71 GDPR, concerning accuracy in the area of profiling.

[111] Article 5(1)(d) GDPR.

must proactively ensure appropriate accuracy, and must offer data subjects the possibility to rectify data.[112]

(5) The storage limitation principle is related to the data minimization principle. Personal data must not be stored for an unreasonably long period.[113] The principle requires that personal data are "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."[114] According to the preamble, storage limitation "requires, in particular, ensuring that the period for which the personal data are stored is limited to a strict minimum."[115] The preamble adds: "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."[116]

(6) The integrity and confidentiality principle could also be called the data security principle. This principle obliges data controllers to ensure "appropriate security" for personal data, "including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."[117]

(7) The accountability principle says that the data "controller shall be responsible for, and be able to demonstrate compliance with" the data principles above.[118] Compared with the Directive, the GDPR puts more emphasis on demonstrating compliance.[119]

### *4.2 The legal basis for processing personal data*

The Charter of Fundamental Rights of the European Union specifies that personal data may only be processed on the basis of the consent of the person concerned or some other legitimate basis, laid down by law.[120] The GDPR specifies that besides consent, there are five other grounds which can be used to legitimate the processing of personal data. The six legal bases are copied almost verbatim from the Directive.[121] Data controllers can base the processing of personal data on any one of these grounds.

---

[112] Article 16 GDPR.
[113] The storage limitation principle adds a nuance: "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 (…) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject." Article 5(1)(e) GDPR.
[114] Article 5(1)(e) GDPR. The storage minimization principle is not explicitly included in the OECD Privacy Guidelines.
[115] Recital 39 GDPR.
[116] Recital 39 GDPR.
[117] Article 5(1)(f) GDPR. See similarly: the Security Safeguards Principle of the OECD Privacy Guidelines.
[118] Article 5(2) GDPR. See similarly: the Accountability Principle of the OECD Privacy Guidelines.
[119] The Article 29 Working Party has promoted the accountability principle since at least 2010. Article 29 Working Party, 'Opinion 3/2010 on the principle of accountability' (WP 173), Brussels, 13 July 2010.
[120] Article 8(2) EU Charter. See also Recital 40. See also: ECJ, C-131/12, Google Spain, 13 May 2014, par 71.
[121] See Article 7 Data Protection Directive.

(1) Processing can be lawful if "the data subject has given consent to the processing of his or her personal data for one or more specific purposes."[122] If a data subject consents to personal data processing, the data protection principles (discussed in the previous section) still apply.[123] For instance, even after the data subject's consent, a controller may not process more personal data than is strictly necessary for the purpose specified.[124] The GDPR defines consent as "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."[125] The GDPR does not accept a consent request that is hidden in terms and conditions: "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."[126] The controller must be able to demonstrate that the data subject has consented to the processing.[127] A data subject can always withdraw his or her consent.[128] Data controllers must ensure that it "shall be as easy to withdraw consent as to give it."[129]

There has been much discussion on whether consent is "freely given" if a company, for instance a social network company, offers a take-it-or-leave-it choice, where people can only use a service if they consent to their data being collected.[130] One example is tracking walls, barriers that website visitors can only pass if they agree to receiving tracking cookies. The GDPR does not outlaw such take-it-or-leave-it choices, but it is not clear that they will be legitimate either.[131] For internet services, children should be at least 16 years old to be able to give valid consent. For children below 16, the parent (or holder of parental responsibility) should authorize consent.[132] The controller should make "reasonable efforts" to verify that consent is given or authorized by the parent,

---

[122] Article 6(1)(a) GDPR.
[123] Article 29 Working Party, 'Opinion 15/2011 on the definition of consent', 01197/11/EN, WP187, 13 July 2011.
[124] See ECJ, C-131/12, Google Spain, 13 May 2014, par 71: "all processing of personal data must comply, first, with the principles relating to data quality set out in Article 6 of the directive [comparable with Article 5 GDPR] and, secondly, with one of the criteria for making data processing legitimate listed in Article 7 of the directive [comparable with the legal bases in Article 6 GDPR]."
[125] Article 4(11) GDPR. See also Recitals 32, 33, 42, and 43 GDPR. See also: Article 29 Working Party, 'Opinion 15/2011 on the definition of consent', 01197/11/EN, WP187, 13 July 2011. The 2012 proposal for a GDPR said that consent had to be "explicit" to be valid. The final text has dropped the word "explicit" from the consent definition. However, the GDPR's requirements for valid consent are so tight that it seems hardly relevant whether the definition requires explicit consent.
[126] Article 7(3) GDPR.
[127] Article 7(1) GDPR.
[128] Article 7(3) GDPR.
[129] Article 7(3) GDPR.
[130] See: Article 29 Working Party 2012, 'Opinion 04/2012 on Cookie Consent Exemption', WP 194, 7 June 2012; Article 29 Working Party, 'Opinion 15/2011 on the definition of consent', 01197/11/EN, WP187, 13 July 2011.
[131] Article 7(4) GDPR.
[132] Article 8(1) GDPR. "Information society services" are, in short, internet services. See Article 4(25) GDPR. See generally on children and consent to data processing: L. Jasmontaite & P. De Hert, *The EU, Children Under 13 Years, and Parental Consent: A Human Rights Analysis of a New, Age-Based Bright-Line for the Protection of Children on the Internet,* 5 International Data Privacy Law 20, 2015.

taking into consideration available technology.[133] The preamble adds that parental consent "should not be necessary in the context of preventive or counseling services offered directly to a child."[134] Member States may provide for a lower minimum consent age, but not lower than 13 years.[135]

(2) The processing of personal data by a data controller can also be legitimate when this is necessary for contract performance. Personal data may be processed if the "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."[136] To illustrate: if somebody orders a pizza at home, the pizzeria can give the customer's address (a piece of personal data) to the delivery man, because the address is "necessary" to deliver the pizza, and thus to perform the contract. For this legal basis to be applicable the processing must be genuinely necessary to perform the contract.[137]

(3) Personal data may also be processed if "necessary for compliance with a legal obligation to which the controller is subject."[138] Say that a national tax law requires companies to keep all records regarding customer transactions for seven years.[139] The pizzeria would be required to store the customer's information for seven years to comply with the tax law's obligation.[140]

(4) Processing can be lawful if "necessary in order to protect the vital interests of the data subject or of another natural person."[141] This legal basis could be invoked, 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."[142]

(5) A controller may process personal data if 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."[143] The legal basis for public authorities to process personal data should

---

[133] Article 8(2) GDPR.
[134] Recital 38 GDPR. See on children also Articles 6(f), 12(1), 17(1)(f), 40(2)(g), 57(1)(b), and Recitals 58, 65, 71, and 75 GDPR.
[135] Article 8(3) GDPR.
[136] Article 6(1)(b) GDPR. See also Recitals 40 and 44 GDPR.
[137] Article 29 Working Party, 'Opinion 06/2014 on the notion of legitimate interests of the data controller under article 7 of Directive 95/46/EC', WP 217, 9 April 2014, p. 17.
[138] Article 6(1)(c) GDPR. The legal obligation should be laid down in the law of the EU or a Member State (Article 6(2) GDPR).
[139] See also Article 29 Working Party, 'Guidelines for Member States on the criteria to ensure compliance with data protection requirements in the context of the automatic exchange of personal data for tax purposes', 175/16/EN, WP 234, 16 December 2015. Article 29 Working Party, 'Statement of the WP29 on automatic inter-state exchanges of personal data for tax purposes', 14/EN, WP 230, 4 February 2015.
[140] Article 29 Working Party, 'Opinion 06/2014 on the notion of legitimate interests of the data controller under article 7 of Directive 95/46/EC', WP 217, 9 April 2014.
[141] Article 6(1)(d) GDPR. See also Recitals 46 and 112 GDPR.
[142] Recital 46 GDPR. See generally: C. Kuner and M. Marelli, Handbook on Data Protection and Humanitarian Action, joint publication of the Brussels Privacy Hub and the International Committee of the Red Cross (ICRC), 30 June 2017 https://shop.icrc.org/handbook-on-data-protection-in-humanitarian-action.html.
[143] Article 6(1)(e) GDPR. See also Recital 45 GDPR.

be laid down in the law of the EU or a Member State.[144] For instance, there might be a national law that says that the state should maintain a database with personal data, registering where citizens live.

(6) Processing is allowed if the controller can rely on the legitimate interests provision, also called the balancing provision.[145] In short, the legitimate interests provision allows processing when it is necessary for the controller's interests, unless the data subject's interests or rights override the controller's interests. In the words of the GDPR: processing is lawful if it 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."[146] The legitimate interests provision is the appropriate legal basis for standard innocuous business practices. For instance, a pizza delivery service may store the customer's address, to send the customer a letter if the pizzeria introduces a new menu, or has a special offer. Storing a customer's name and address does not, in general, heavily infringe privacy, and the pizzeria has a legitimate interest in promoting its own business. The pizzeria would probably pass the balancing test prescribed by the legitimate interests provision.[147]

Whether a controller can rely on the legitimate interests provision depends on the circumstances.[148] Compared to the Directive, the GDPR gives more guidance on how to apply the legitimate interests provision.[149] New in the GDPR is the explicit requirement that the controller must, in principle, inform the data subject of the interests for which it processes personal data.[150] The phrase "in particular where the data subject is a child" in the legitimate interests provision is also new. Unlike the Directive, the GDPR states explicitly that public authorities should not rely on the legitimate interests provision as "it is for the legislator to provide by law for the legal basis for public authorities to process personal data."[151] If a data controller relies on the legitimate interests provision for processing, the data subject has, in principle, a right to object to (opt out of) the processing.[152]

---

[144] Article 6(2) GDPR.
[145] Article 6(1)(f) GDPR. See also Recitals 47-50 GDPR.
[146] Article 6(1)(f) GDPR.
[147] See further: CJEU, Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde v Rīgas pašvaldības SIA 'Rīgas satiksme', C-13/16, 4 May 2017.
[148] See Recitals 10, 47, 48, and 49 GDPR. The Article 29 Working party has published a detailed opinion on the legitimate interests provision. Article 29 Working Party, 'Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC', 844/14/EN, WP 217, 9 April 2014.
[149] Recitals 37, 47 and 49 GDPR.
[150] Article 13(1)(d) GDPR.
[151] Recital 47 GDPR.
[152] Article 21 GDPR.

### *4.3 The processing of special categories of personal data*

The GDPR retains a stricter regime for certain "special categories" of personal data, sometimes called sensitive data.[153] Like in the Directive, processing special data categories is prohibited, unless an exception applies. Both the Directive and the GDPR specify that the processing of personal data revealing racial or ethnic origin,[154] political opinions,[155] religious or philosophical beliefs, or trade-union membership, and the processing of genetic data,[156] biometric data[157] for the purpose of uniquely identifying a natural person,[158] data concerning health,[159] or data concerning a natural person's sex life or sexual orientation shall be prohibited.[160] The Court of Justice of the European Union has adopted a wide interpretation of these classes. For example, it decided that reference to the fact that an individual has injured her foot and works part-time on medical grounds constitutes personal data concerning health.[161]

The GDPR in principle prohibits the processing of special categories of data, but also includes a number of exceptions to this rule.[162] While the Data Protection Directive only mentioned five situations in which this prohibition did not apply, the GDPR mentions ten.

(1) By giving their "explicit" consent, data subjects can override the prohibition on processing special data categories.[163] Member States may opt for a regime where the data subject cannot override the prohibition with consent.[164]

(2) When processing is necessary in relation to the obligations in the field of employment and social security and social protection law.[165]

(3) When 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.[166]

---

[153] See also Recitals 10, 34, 35, 50-65, 71, 91, 97 GDPR.
[154] Regarding data about racial origin, the preamble says that the EU does not accept theories that try to determine the existence of separate human races (Recital 51 GDPR).
[155] See on personal data revealing political opinions: Recital 56 GDPR.
[156] See on genetic data: Article 4(13) GDPR. Recital 34 GDPR.
[157] Article 4(14) GDPR. Dactyloscopic data are, in short, fingerprint data. Recital 51 GDPR.
[158] See on biometric data: Recitals 51 and 53 GDPR.
[159] See on data relating to health: Recitals 35, 45, 52-54, 63, 65, 71, 75, 91 GDPR. Health data can relate to both a person's physical and mental health, including the provision of health care services, which reveal information about his or her health status. Article 4(15) GDPR.
[160] Article 9(1) GDPR. Footnotes added by the authors.
[161] ECJ, Bodil Lindqvist, Case C-101/01, 6 November 2003.
[162] The Data Protection Directive had a similar regime in Article 8 Data Protection Directive.
[163] Article 9(2)(a) GDPR.
[164] Article 9(2)(a) GDPR.
[165] Article 9(2)(b) GDPR. Recital 52 GDPR.
[166] Article 9(2)(c) GDPR.

(4) When the data subjects are members of a church, trade union, political party, or similar non-profit organisation, that organisation may process special categories of data that are necessary for its functioning.[167]

(5) If a data subject has manifestly made his or her personal data public, the prohibition of processing special categories of data does not apply.[168]

(6) When processing is necessary for the establishment, exercise, or defense of legal claims or whenever courts are acting in their judicial capacity.[169]

(7) When processing is necessary for reasons of substantial public interest.[170] Hence, the GDPR adds an additional requirement when it comes to legitimizing the processing of special categories of data. The processing should not only be in the public interest, but in the "substantial" public interest. The GDPR does not specify what is to be regarded as substantial.

(8) When processing is necessary for preventive or occupational medicine. This ground typically plays a role within employer-employee relations. For example, when the processing of health data is necessary 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.[171]

(9) When processing is necessary for a specific public interest, which should be presumed to be a "substantial public interest", namely when the processing of special categories of data is necessary in the area of public health. Examples include 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.[172]

(10) Finally, under certain circumstances processing can be allowed when the processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.[173]

Like the Directive, the GDPR contains a separate regime for personal data relating to criminal convictions and offences. In brief, only an official authority may process personal data relating to criminal convictions and offences or related security measures. A comprehensive register of criminal convictions may only be kept under the control of official authority.[174]

---

[167] Article 9(2)(d) GDPR.
[168] Article 9(2)(e) GDPR.
[169] Article 9(2)(f) GDPR.
[170] Article 9(2)(g) GDPR.
[171] Article 9(2)(h) GDPR.
[172] Article 9(2)(i) GDPR.
[173] Article 9(2)(j) GDPR. See also Article 89 GDPR.
[174] Article 10 GDPR.

### *4.4 Cross-border data transfers*

The EU is not only ambitious with respect to the regulation of the processing of personal data by European organizations and companies. As mentioned, the GDPR also applies to data controllers and processors that are based outside the EU, if they offer goods or services to data subjects in the Union, irrespective of whether a payment of the data subject is required, or when they use personal data for monitoring the behavior of EU citizens as far as their behavior takes place within the Union. But the GDPR also regulates the data flows to countries outside the EU.[175] Such transfer is only allowed in three situations.

(1) When there is a so-called adequacy decision by the European Commission, data transfers can be deemed legitimate. The Commission can declare that it is safe to send personal data from the EU to a certain country, subject to potential restrictions and limitations, when it is believed that that country offers a sufficiently high level of data protection.[176] So far, the Commission has only issued such a decision with respect to twelve territories: [177] Andorra, Argentina, Canada, Switzerland, Faeroe Islands, Guernsey, State of Israel, Isle of Man, Jersey, New Zealand, United States, and Eastern Republic of Uruguay.[178]

The recent Schrems decision by the European Court of Justice has complicated this situation. The European Court of Justice invalided the Safe Harbor agreement,[179] which served as an adequacy decision of the European Commission.[180] Inter alia, the Court held:

> In particular, legislation permitting the public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life, as guaranteed by Article 7 [the right to privacy] of the Charter. Likewise, legislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him, or to obtain the rectification or erasure of such data, does not respect the essence of the fundamental right to effective judicial protection, as enshrined in Article 47 of the Charter. The first paragraph of

---

[175] Article 44 GDPR.
[176] Article 45 GDPR.
[177] These adequacy decisions do not cover data exchanges in the law enforcement sector. For special arrangements concerning exchanges of data in this field: http://ec.europa.eu/justice/data-protection/international-transfers/pnr-tftp/pnr-and-tftp_en.htm
[178] http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm
[179] Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46 on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce
[180] See also: Article 29 Working Party, 'Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision', 16/EN, WP 238, 13 April 2016. Article 29 Working Party, 'Statement of the Article 29 Working Party', 16 October 2015.

> Article 47 of the Charter requires everyone whose rights and freedoms guaranteed by the law of the European Union are violated to have the right to an effective remedy before a tribunal in compliance with the conditions laid down in that article. The very existence of effective judicial review designed to ensure compliance with provisions of EU law is inherent in the existence of the rule of law.[181]

Following that decision, the European Commission has negotiated a new agreement with the US, called the Privacy Shield,[182] in which some of the concerns raised by the Court of Justice have been addressed. However, other points of concern seem to remain. Indeed, the new adequacy decision has been challenged before the Court as well.[183]

(2) If no adequacy decision applies, transfer of personal data may be allowed if there are appropriate safeguards. Those safeguards should ensure compliance with data protection requirements and the rights of the data subjects, 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. The safeguards should relate in particular to compliance with the general principles relating to personal data processing, and 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 organizations 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. Authorization from the competent supervisory authority should be obtained when the safeguards are provided for in administrative arrangements that are not legally binding.[184] There are several ways in which appropriate safeguards can be applied.[185]

1. When it concerns cross border data sharing between public authorities or bodies and there is a legally binding and enforceable instrument in place that regulates the sharing of data. The Court of Justice of the European Union has stressed that it is not permissible to implement national measures which allow a public administrative body of a Member State to transfer personal data to another public administrative body and their subsequent processing, without the data subjects having been informed of that transfer or processing.[186]

---

[181] Court of Justice, Maximillian Schrems v Data Protection Commissioner, Case C-362/14, 6 October 2015.

**[182]** Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield (notified under document C(2016) 4176).

[183] Action brought on 16 September 2016 – Digital Rights Ireland v Commission (Case T-670/16), http://curia.europa.eu.

[184] Recital 108 GDPR.

[185] Article 46 GDPR.

[186] CJEU, Smaranda Bara and Others v Președintele Casei Naționale de Asigurări de Sănătate, Casa Națională de Asigurări de Sănătate, Agenţia Naţională de Administrare Fiscală (ANAF), Case C-201/14, 1 October 2015.

2. When there are "binding corporate rules". Such rules should be legally binding and apply to every member concerned of the group of undertakings and such rules should expressly confer enforceable rights on data subjects with regard to the processing of their personal data. In addition, the binding corporate rules should, inter alia, include the structure and contact details of the group of undertakings, the data transfers or set of transfers, their legally binding nature, both internally and externally, how the data protection obligations are implemented, how the rights of the data subject will be respected, how the information on the binding corporate rules is provided to the data subjects, the tasks of any data protection officer designated, and the complaint procedures.[187]
3. When the Commission has adopted standard data protection clauses or when a supervisory authority has done so.[188] Using such clauses should not prevent controllers or processors 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 the standard contractual clauses or prejudice the fundamental rights or freedoms of the data subjects. Rather, the GDPR stresses that controllers and processors are encouraged to provide additional safeguards via contractual commitments that supplement standard protection clauses.[189]
4. When there is an approved code of conduct together with binding and enforceable commitments for the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights.
5. When there is an approved certification mechanism together with binding and enforceable commitments for the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights.

(3) If no adequacy decision applies and no appropriate safeguards have been adopted, there are grounds on the basis of which the prohibition on the transfer of personal data to third countries can be exempted. These grounds align with the legal basis for data processing discussed in sections 4.1 and 4.2. The derogations can only legitimize data transfer in specific situations, for a single or small set of transfer(s) of personal data to third countries. They cannot be used to legitimize more structural data transfers. The GDPR mentions eight such derogations.[190]

1. The data subject has explicitly consented to the 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. A disadvantage for the controller is that data subjects can always withdraw their consent.[191]

---

[187] Article 47 GDPR. See: Moerel L, *Binding Corporate Rules: Corporate Self-regulation of Global Data Transfers (PhD thesis University of Tilburg)* 2011.
[188] Article 93(2) GDPR. Article 5 of Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by Member States of the Commission's exercise of implementing powers.
[189] Recital 109 GDPR.
[190] Article 49 GDPR.
[191] Article 7(3) GDPR.

2. The transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request.
3. 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.
4. The transfer is necessary for important reasons of public interest. Examples include cases of international data exchange between competition authorities, tax or customs administrations, financial supervisory authorities, services competent for social security matters, or for public health, for instance in the case of contact tracing for contagious diseases or to reduce doping in sport.[192]
5. The transfer is necessary for the establishment, exercise, or defense of legal claims.
6. The transfer is necessary 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.
7. The transfer is made from a register which according to Union or Member State law is intended to provide information to the public.[193]
8. Where a transfer cannot be based on an adequacy decision or appropriate safeguards, and none of the derogations listed above apply, a transfer 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.

## 5. RESPONSIBILITIES FOR DATA CONTROLLERS AND PROCESSORS

As mentioned, the definitions of the data controller and data processor have remained mostly the same in the GDPR. But in relation to their responsibilities, quite some changes have been made. For example, the responsibilities of the "processor" have been elaborated.[194] Data controllers may only contract with processors that provide sufficient technical and organizational measures to protect personal data and the rights of data subjects. Moreover, the relationship between the controller and the processor must be laid down in a contract, which must contain, inter alia, clauses specifying that processors can only process personal data on the explicit and documented instruction

[192] Recital 112 GDPR.
[193] See also Article 49.2 GDPR.
[194] Article 28 GDPR.

of the controller and that the processor shall process the data in a confidential manner.[195]

These rules seem to reaffirm the position of the data controller as the party primarily responsible for upholding the data protection principles. This responsibility is underlined, among others, by the provision holding that data processors may only hire or contract other persons to process the data with the explicit consent of the data controller. The GDPR specifies that if the 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.[196]

The GDPR clarifies that where two or more controllers jointly determine the purposes and means of the processing of personal data, they are joint controllers. These parties must, in a transparent manner, determine their responsibilities, in particular as regards the exercising of the rights of the data subject and their duties to provide information to data subjects.[197] The data subject may exercise his or her rights against each of the controllers.[198] Although these rules provide a bit more clarity, the GDPR leaves it primarily up to the data controllers to make agreements on their joint responsibilities. This seems a clear and effective solution when, for example, two companies of equal size work together and harvest a combined dataset. With regard to internet platforms that use "user generated content" (such as YouTube), however, it is less clear how this solution will work.[199] Internet platforms may try to shift as much responsibility as possible towards the users of their platforms. However, it is questionable whether under EU law, such one-sided "agreements" enforced by market leaders and monopolists would be valid. It remains to be seen how this will work out in practice.

Regarding the responsibilities of data users, the GDPR includes a general provision with respect to the responsibility of the data controller, specifying that the controller must implement appropriate technical and organizational measures to ensure and be able to demonstrate that the processing of personal data is performed in compliance with the rules. These measures can be reviewed and updated where necessary and proportionate in relation to the processing activities, and shall include the implementation of appropriate data protection policies by the controller.[200]

Additionally, a definition of the "representative" is included in the GDPR.[201] The GDPR specifies that the representative shall be mandated by the controller or the 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

---

[195] See also Recital 81 GDPR.
[196] See also: Article 29 GDPR.
[197] Article 29 Working Party, 'Opinion 1/2010 on the concepts of "controller" and "processor"', 00264/10/EN WP 169, Brussels, 2010.
[198] Article 26.2 GDPR.
[199] See: D. Erdos, *Delimiting the Ambit of Responsibility of Intermediary Publishers for Third Party Rights in European Data Protection: Towards a Synthetic Interpretation of the EU acquis* (June 27, 2017). University of Cambridge Faculty of Law Research Paper No. 31/2017. https://ssrn.com/abstract=2993154.
[200] Article 24 GDPR.
[201] Article 4(17) GDPR.

personal data processing, for the purposes of ensuring compliance with the GDPR.[202] Data controllers must appoint a representative if they are not based in the European Union but fall under the territorial scope of the GDPR.[203] The representative is thus meant as a point of contact for third parties in relation to data protection questions. This position was already required in the Directive,[204] but has now been clarified.[205]

Below, we discuss six requirements for data users. First, they must document data processing initiatives and second, they must be transparent. Third, they must implement technical measures to ensure that the data processing is conducted safely and confidentially. Fourth, in specific circumstances they must inform the Data Protection Authority of their operations. Fifth, under certain circumstances data users must appoint a data protection officer, who is responsible for adequate data protection standards and procedures within an organization. Sixth, under certain circumstances, they must execute a Data Protection Impact Assessment, through which they assess the potential impact of the data processes they conduct on citizens or society as a whole. Then there are two optional mechanisms, namely adopting codes of conduct and a certification mechanism.

### *5.1 Documentation*

The GDPR introduces a general obligation for data controllers to keep records of their processing activities.[206] This record shall include: the name and contact details of the controller; the processing purposes; a description of categories of data subjects and of the categories of personal data; the categories of recipients to whom the personal data have been or will be disclosed;[207] transfers of data to a third country;[208] the envisaged time limits for erasure of the different categories of data; and (where possible) a general description of the technical and organizational security measures. This obligation to keep records aims to ensure that controllers can be held accountable for breaching data protection principles.[209] The onus lies principally on controllers to provide either a judge or a Data Protection Authority with detailed information to show that they have acted carefully and legitimately.

The Directive contained a provision requiring a data controller to notify the Data Protection Authority when it was planning to process personal data.[210] This would allow Data Protection Authorities to keep a register of data processing activities and to

---

[202] Article 27(4) GDPR.
[203] Article 3(2) GDPR.
[204] Article 4 Data Protection Directive.
[205] See also Recital 80 GDPR.
[206] Article 30 GDPR.
[207] Smaller enterprises are exempted from this rule – the exemption has been included out of economic motives. Recital 13 GDPR.
[208] Recital 48 GDPR holds: "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."
[209] See also Recital 82 GDPR.
[210] Article 18 and 19 Data Protection Directive.

assess the proposed initiatives beforehand or intervene at an early stage. However, most Data Protection Authorities suggested that it was unfeasible for them to keep a record of all different initiatives, let alone assess them beforehand. Consequently, this obligation has been deleted and replaced by an obligation to notify a Data Protection Authority if a data breach has occurred (even when this has no significant effect on any data subject).[211]

### *5.2 Transparency*

The GDPR requires data controllers to demonstrate transparency regarding their processing activities.[212] Controllers not only have an obligation to respond to the requests of data subjects, but also have an independent transparency obligation. Failing to comply, even without any data subject having requested information, is an independent infringement of the data protection principles and can lead to fines.

In connection with the purpose limitation principle, the GDPR specifies that when the controller intends to further process the data for a purpose other than the one for which the data were collected, the data subject must be informed of that intent.[213]

The GDPR takes into account the fact that it may be difficult for data controllers to contact data subjects. The GDPR specifies that where the data controller obtains personal data that is not directly from the data subject, it is absolved from the transparency obligation in a number of situations. For instance, the controller does not have to provide information when: the data subject already has the information; the provision of such information proves impossible or would involve a disproportionate effort; obtaining or disclosure is laid down by a law that provides appropriate measures to protect the data subject's legitimate interests; or the data must remain confidential because of professional secrecy regulated by law.[214]

The GDPR requires data controllers to provide information “in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child.”[215] The GDPR specifies a time frame to respond to requests by data subjects and a duty to explain immediately when a request by a data subject is denied.[216]

More specifically, there is a duty to inform the data subject if a data breach has occurred. The e-Privacy Directive already contained such a rule for activities falling under its scope.[217] The GDPR defines a data breach as “"a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or

---

[211] Article 33 GDPR.
[212] Article 12-14 GDPR.
[213] Article 13-14 GDPR.
[214] Article 14 GDPR.
[215] Article 12 GDPR.
[216] Article 12(2) and 12(4) GDPR.
[217] Article 4 e-Privacy Directive.

access to, personal data transmitted, stored or otherwise processed".[218] When such a data breach occurs and is likely to result in a high risk for the rights and freedoms of individuals, the controller must communicate this to the data subject without undue delay.[219] Such a high risk is not said to exist when the data controller has used effective encryption or other effective techniques.[220]

The duty to inform specific data subjects does not exist when this would mean a disproportionate effort for the data controller. In such a case, the controller must inform data subjects through a public communication or similar measure.[221]

### *5.3 Technical measures*

Data users must ensure appropriate security when processing personal data. The GDPR specifies in detail what the security measures must entail. Pointing to the state of the art and the costs of implementation, the GDPR holds that the controller and the processor shall implement appropriate technical and organizational measures, taking into account the nature, scope, context, and purposes of the processing as well as the risks of varying likelihood and severity for the rights and freedoms of individuals. Such security measures can include: pseudonymization and encryption; the ability to ensure the ongoing confidentiality; integrity, availability, and resilience of systems and services processing personal data; the ability to restore the availability and access to data in a timely manner in the event of a physical or technical incident; and a process for regularly testing, assessing, and evaluating the effectiveness of security measures.[222]

The GDPR broadens its focus on technical design. The GDPR differentiates between privacy by design and privacy by default – called data protection by design and data protection by default in the GDPR. Data protection by design broadly means that privacy rules are implemented in the technical infrastructure. Data protection by default indicates that privacy-enhancing choices are made the default in the technical infrastructure, while data subjects can change the default. With respect to data protection by design, the GDPR specifies that the controller shall, both at the time of the determination of the means for processing and during the processing, implement appropriate technical and organizational measures, such as pseudonymization and data minimization.[223] The controller does not have to aim for absolute security: security measures must be appropriate having regard to the state of the art and the cost of implementation and taking account of the nature, scope, context, and purposes of the

---

[218] Article 4(12) GDPR. See also: Article 29 Working Party, 'Opinion 03/2014 on Personal Data Breach Notification', 693/14/EN, WP 213, 25 March 2014. Article 29 Working Party, 'Opinion 06/2012 on the draft Commission Decision on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC on privacy and electronic communications', 01119/13/EN, WP197, 12 July 2012.
[219] Article 34 Data Protection Directive.
[220] See also Recital 83 on this point and Recitals 85-88 GDPR on the data breach point.
[221] See further: Article 29 Working Party, 'Opinion 03/2014 on Personal Data Breach Notification', 693/14/EN, WP 213, 25 March 2014.
[222] Article 32 GDPR.
[223] Article 25(1) GDPR.

processing, as well as the risks of varying likelihood and severity for rights and freedoms of individuals posed by the processing.[224]

With respect to data protection by default, the GDPR specifies that the controller shall implement appropriate technical and organizational measures for ensuring that, by default, only personal data that are necessary for each specific purpose of the processing are processed. 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 individuals.[225]

### *5.4 Notifying the Data Protection Authority*

Perhaps the biggest innovation the GDPR brings about with respect to the duties of data controllers concerns organizational measures they have to implement. There are several aspects of particular relevance in this respect. The Directive specified that the controller must notify the supervisory authority before carrying out any wholly or partly automatic processing operation or set of such operations intended to serve a single purpose or several related purposes.[226] This allowed Data Protection Authorities to assess these plans and intervene at an early stage, when processing operations are likely to present specific risks to the rights and freedoms of data subjects.[227] However, the Directive allowed Member States to limit this duty.[228] Many states have indeed done so. In 2010, the European Commission also pointed to the administrative burden and stated: "A further concrete element for lessening the administrative burden and reducing costs for data controllers would be the revision and simplification of the current notification system."[229] Indeed, the obligation to notify the Data Protection Authority of processing has been deleted in the GDPR.

Only under specific circumstances, for instance when there has been a data breach, must the data controller inform the Data Protection Authority. As mentioned, when there is a data breach that may have a big impact on a data subject, the data controller has to inform the person in question. But more generally, when there is a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the competent supervisory authority, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.[230]

---

[224] See on the notion of risk Recital 76 GDPR.
[225] Article 25(2) GDPR.
[226] Article 18 Data Protection Directive.
[227] Article 20 Data Protection Directive.
[228] Article 19 Data Protection Directive.
[229] A comprehensive approach on personal data protection in the European Union, Brussels, 4.11.2010 COM(2010) 609 final, p. 10. See also: Report from the Commission - First report on the implementation of the Data Protection Directive (95/46/EC) /* COM/2003/0265 final, p. 18. <http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52003DC0265&from=LV>.
[230] Article 33 GDPR.

### *5.5 Data protection officer*

The Directive already mentioned the possibility for organizations to appoint a data protection official within their organization, though this was voluntary.[231] In practice, even if an organization did appoint such an official, he or she was often unequipped and underfinanced to fulfil the tasks, and the independence of the officer vis-à-vis the directors of an organization was often not guaranteed. Also, there was a large variation in the official tasks and competences of the officials in the laws of the different EU Member States. [232] In 2010, the European Commission suggested making "the appointment of an independent Data Protection Officer mandatory and harmonising the rules related to their tasks and competences, while reflecting on the appropriate threshold to avoid undue administrative burdens, particularly on small and micro-enterprises."[233]

The GDPR specifies that the controller and the processor shall designate a data protection officer in three circumstances.[234] First, where a public authority carries out the processing, except for courts acting in their judicial capacity. [235] Second, when the core activities of the controller or the processor consist of processing operations that require regular and systematic monitoring of data subjects on a large scale. Third, when the core activities of the controller or the processor consist of processing special categories of data on a large scale.[236]

The GDPR requires that the officer is fully equipped, fully informed about all data processing activities, and fully independent.[237] The tasks of the data protection officer include: informing and advising the controller or the processor of their obligations; monitoring compliance with the GDPR; providing advice regarding the Data Protection Impact Assessment; cooperating with the Data Protection Authority; and acting as the contact point for the Data Protection Authority.[238]

### *5.6 Data protection impact assessments*

The GDPR specifies that under certain circumstances data controllers must do a Data Protection Impact Assessment,[239] before engaging in the planned processing. The idea of doing impact assessments is inspired by environmental law. The GDPR specifies that the controller shall, prior to the processing, carry out a Data Protection Impact

---

[231] Article 18 and 20 Data Protection Directive.
[232] See also: CJEU (Grand Chamber), Volker und Markus Schecke GbR (C-92/09), Hartmut Eifert (C-93/09) v Land Hessen, Joined Cases C-92/09 and C-93/0, 9 November 2010.
[233] A comprehensive approach on personal data protection in the European Union, Brussels, 4.11.2010 COM(2010) 609 final, p. 12.
[234] See also Recital 97 GDPR.
[235] See further: EDPS, 'Position paper on the role of Data Protection Officers in ensuring effective compliance with Regulation (EC) 45/2001', Brussels, 28 November 2005.
[236] Article 37 GDPR.
[237] Article 38 GDPR.
[238] Article 39 GDPR.
[239] See also: Article 29 Working Party, 'Opinion 04/2013 on the Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems ('DPIA Template') prepared by Expert Group 2 of the Commission's Smart Grid Task Force', 00678/13/EN, WP205, 22 April 2013.

Assessment if a type of processing is likely to result in a high risk for the rights and freedoms of individuals.[240]

Such a Data Protection Impact Assessment is required in three cases in particular: when a systematic and extensive evaluation of personal aspects is based on automated processing or profiling and leads to decisions that significantly affect the individual, when special categories of data are processed on a large scale, and when systematically monitoring a publicly accessible area on a large scale.[241] Such an assessment must contain at least a systematic description of the envisaged processing operations and the purposes of the processing, an assessment of the necessity and proportionality of the processing operations, and an assessment of the risks to the rights and freedoms of data subjects and the measures envisaged to address the risks. Data controllers must consult the Data Protection Authority prior to the processing of personal data where a Data Protection Impact Assessment indicates that the processing would result in a high risk. Where the Data Protection Authority thinks that the intended processing would not comply with the GDPR, it shall give advice on how to mitigate the risks.[242]

### *5.7 Codes of conduct*

The Directive already included the possibility of drawing up codes of conduct. A code of conduct was a non-mandatory, primarily sectorial instrument, aimed at trade associations or bodies representing a certain sector as a whole.[243] The idea was that these bodies would fine-tune the codes when discussing them with Data Protection Authorities and that these codes could specify how the, rather general, data protection rules in the Directive should be interpreted in certain sectors and situations. Although there are differences from country to country, generally codes of conduct are not widely used.[244]

The rules in the GDPR regarding codes of conduct have mostly remained the same.[245] New is that the monitoring of compliance with a code of conduct 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 this purpose by the competent Data Protection

---

[240] Article 35(1) GDPR.
[241] Article 35(1) – 35 (3) GDPR. See also Recitals 89-94 GDPR.
[242] Article 36 GDPR.
[243] Article 27 Data Protection Directive.
[244] In 2010, the Commission remarked: "The Commission continues to consider that self-regulatory initiatives by data controllers can contribute to a better enforcement of data protection rules. The current provisions on self-regulation in the Data Protection Directive, namely the scope for drawing up Codes of Conduct, have rarely been used so far and are not considered satisfactory by private stakeholders. Furthermore, the Commission will explore the possible creation of EU certification schemes (e.g. 'privacy seals') for 'privacy-compliant' processes, technologies, products and services." A comprehensive approach on personal data protection in the European Union, Brussels, 4.11.2010 COM(2010) 609 final, p. 12. The Commission, in 2003, explicitly marked its disappointment on this matter: "The Commission is disappointed that so few organisations have come forward with sectoral Codes of Conduct for application at Community level." Report from the Commission - First report on the implementation of the Data Protection Directive (95/46/EC) /* COM/2003/0265 final**,** p. 26. <http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52003DC0265&from=LV>.
[245] Article 40 GDPR.

Authority.[246] Data Protection Authorities also remain competent. This new rule may relieve Data Protection Authorities in part from their duties and responsibilities.[247]

### *5.8 Certification mechanism*

The GDPR introduces a new certification scheme. The GDPR tries to promote self- and co-regulation. In doing so, the GDPR shifts responsibilities and regulatory burdens from the Data Protection Authorities to the data controllers. A recital specifies that in "order to enhance transparency and compliance with this Regulation, the establishment of certification mechanisms, data protection seals and marks should be encouraged, allowing data subjects to quickly assess the level of data protection of relevant products and services."[248] How this will work in practice is not yet clear.

The GDPR encourages the establishment of data protection certification mechanisms and of data protection seals and marks. These may also be established for demonstrating the existence of appropriate safeguards provided by controllers or processors that are not subject to the GDPR. The certification shall be voluntary and available via a process that is transparent. A certification shall be issued by the certification body or by the competent supervisory authority on the basis of the criteria approved by the competent supervisory authority or the European Data Protection Board. In the latter case, the criteria approved by the European Data Protection Board may result in a common certification: the European Data Protection Seal.[249] Certification bodies must have an appropriate level of expertise in relation to data protection. [250] They may be accredited by the Data Protection Authority or the National Accreditation Body.[251]

In conclusion, the GDPR contains more detailed requirements regarding the responsibilities of data controllers and processors.

## 6. RIGHTS OF THE DATA SUBJECT

The GDPR aims to empower data subjects by granting them various rights, such as the right to access, rectify, and erase personal data, and the right to object to, or restrict, processing. Compared with the Directive, the GDPR provides more detail regarding the data subject's rights. In short, when processing personal data, in order to be compliant under the GDPR data controllers have to respect seven rights of the data subject: the right to access; to data portability; to rectify data; to stop processing; to object; to erase data; and to resist profiling.

---

[246] Article 41 GDPR.
[247] See also Recitals 98 and 99 GDPR.
[248] Recital 100 GDPR.
[249] Article 42-43 GDPR.
[250] Article 43 GDPR. See generally: R. Rodrigues, D. Barnard-Wills, P. De Hert, V. Papakonstantinou, *The future of privacy certification in Europe: an exploration of options under article 42 of the GDPR* (2016) 30(3) International Review of Law, Computers & Technology 248.
[251] Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93.

### *6.1 The right to access personal data*

Everyone has the right to access his or her personal data, says the Charter of Fundamental Rights of the European Union.[252] The GDPR elaborates: "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."[253] The data subject also has the right to obtain additional information, for instance about the processing purposes, the categories of personal data concerned, the storage period, the recipients to whom the personal data have been or will be disclosed, and information about where the controller obtained the data.

Upon an access request, the controller must provide a copy of the personal data undergoing processing.[254] For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs.[255] The explicit requirement for a copy is new in the GDPR.[256] The right to obtain a copy must not adversely affect the rights and freedoms of others.[257] If the data subject makes the request by electronic means, in principle the controller must provide the data in a commonly used electronic form.[258] This provision must be interpreted, according to the Court of Justice of the European Union, as not precluding the levying of fees in respect of the communication of personal data by a public authority. However, the fees levied when the right to access personal data is exercised should not exceed the cost of communicating such data.[259]

### *6.2 Right to data portability*

The GDPR extends the right to access one's data, by introducing the right to data portability, which is supposed to strengthen the data subject's control over personal data.[260] The right to data portability seems to be inspired by the right to number portability, which granted the consumer a right to maintain his telephone number when changing providers.[261] Under the GDPR's right to data portability, the data subject can take his data from one platform, for example Facebook, to another platform, for

---

[252] Article 8(2) EU Charter. See also Recitals 60-64 GDPR.
[253] Article 15(1) GDPR.
[254] Article 15(3) GDPR.
[255] Article 15(3) GDPR. See also Recital 59 GDPR.
[256] See: CJEU, YS. and M. and S. v. Minister of Immigration, Integration and Asylum, C-141/12 and C-372/12, 17 July 2014, and on that case: E.R. Brouwer and F.J. Zuiderveen Borgesius (joint first author), *Access to personal data and the right to good governance during asylum procedures after the CJEU's YS and M. and S. judgment*, European Journal of Migration and Law 2015-7, p. 259-272.
[257] Article 15(4) GDPR.
[258] Article 15(3) GDPR: "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." Under certain circumstances, data controllers must inform data subjects about access, rectification, and erasure rights (Article 13(2)(b) and Article 14(2)(c) GDPR).
[259] CJEU, X, C-486/12, 12 December 2013.
[260] Recital 68 GDPR.
[261] The Universal Services Directive (2002/22/EC) requires phone companies to offer number portability (Article 30(1)).

example another social network site.[262] This right to data portability only applies to personal data that the data subject has provided himself. The data controller must provide such data to the data subject (or to a third party on the request of the data subject) in a structured, commonly used, and machine-readable format.[263]

The data subject has the right to have the personal data transmitted directly from one controller to another, where technically feasible.[264] The preamble adds that the data portability right does not oblige "controllers to adopt or maintain processing systems which are technically compatible."[265]

The right to data portability applies when the processing (i) is based on the data subject's consent, or on the legal basis of necessity for contract performance, and (ii) the processing is carried out by automated means.[266] The right to data portability does not apply to processing necessary for a task carried out in the public interest or in the exercise of official authority vested in the controller.[267] The right to data portability shall be without prejudice to the right to erasure,[268] and must not "adversely affect the rights and freedoms of others."[269]

### *6.3 The right to rectify personal data*

Data subjects also have the right to rectify inaccurate personal data that concern them.[270] The right to rectification is also granted in the Charter of Fundamental Rights of the European Union.[271] Taking into account the processing purposes, the data subject has the right to have incomplete personal data completed, for instance by adding a supplementary statement. The explicit mention of supplementary information is new in the GDPR.

The right to rectification can be useful, for instance, for credit reports. As noted, inaccurate data in a credit report can cause many problems. Adding a supplementary statement could be useful, for instance, when somebody did not pay a phone bill because the phone provided by a company did not function. If a credit report merely says "missed payments", a supplementary statement about the reason for non-payment could be appropriate.

---

[262] Article 20 GDPR.
[263] Article 20(1) GDPR.
[264] Article 20(2) GDPR.
[265] Recital 68 GDPR.
[266] Article 20(1) GDPR.
[267] Article 20(3) GDPR.
[268] Article 20(3) GDPR.
[269] Article 20(4) GDPR. See generally on the GDPR's right to data portability: P. Swire and L. Yianni, *Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique*, *Md. L. Rev.* 72 (2012): 335; B. Engels, *Data Portability among Online Platforms,* 5 Internet Policy Review (2016).
[270] Article 16 GDPR.
[271] Article 8(2) of the Charter of Fundamental Rights of the European Union.

### *6.4 Rights to stop processing*

There are three rights that the data subject can invoke to stop the processing of his personal data, in whole or in part. These are the right to restrict processing (discussed in this section), the right to object to processing, and the right to erasure (discussed below). First, data subjects have the right to "restrict" processing, a new concept in the GDPR. The "restriction of processing" is defined as "the marking of stored personal data with the aim of limiting their processing in the future."[272] A restriction on processing could be seen as a processing pause, while details about the fairness and lawfulness of a processing activity are examined.

A data subject can demand the restriction of profiling, for example, in the following circumstances. If the data subject contests the data's accuracy, he or she can demand restriction for a period enabling the controller to verify the accuracy of the personal data. The data subject can also demand a restriction on processing if the processing is unlawful. The right applies as well if the controller no longer needs the personal data for the purposes of the processing, but the data subject requires the data for exercising legal claims. The data subject can also demand restriction if he or she has objected to processing pending the verification of whether the legitimate grounds of the controller override those of the data subject.[273]

Where processing has been restricted, the personal data may only be processed with the data subject's consent, for legal reasons, or for an important public interest.[274] Before the controller lifts a restriction of processing, the controller must inform the data subject who has obtained the restriction of processing.[275]

### *6.5 Right to object*

The GDPR grants data subjects a right to object to processing on grounds relating to their particular situation.[276] If a controller relies on the legal basis of necessity for a public interest or on the legitimate interests provision,[277] data subjects have a right to object. The data controller must explicitly bring the objection right to the attention of the data subject.[278] If a data subject exercises the right to object, in principle the controller must stop the processing.

But the right to object is not absolute. After a data subject objects, the controller may continue the processing if the controller demonstrates compelling legitimate grounds for the processing that override the interests of the data subject, or for exercising legal

---

[272] Article 4(3) GDPR. See also Recital 65 GDPR.
[273] Article 18(1) GDPR.
[274] Article 18(2) GDPR.
[275] Article 18(3) GDPR.
[276] Article 21(1) GDPR.
[277] Article 6(1)(2) and 6(1)(f) GDPR.
[278] Article 21(4) GDPR.

claims.[279] A state body that processes personal data can override a data subject objection for reasons of public interest.[280]

The data subject has an absolute right to object in the case of direct marketing: "Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes."[281] That absolute right to object could be seen as a right to opt out of direct marketing.

Hence, the GDPR distinguishes between opt-in systems for direct marketing (based on consent) and opt-out systems for direct marketing (the right to object). In some cases, direct marketing can only be based on the data subject's consent. For instance, personal data processing for behavioral advertising[282] generally requires the data subject's consent.[283] In some, more innocuous, cases, companies can process personal data for direct marketing without the data subject's consent, based on the legitimate interests provision.[284] For instance, data processing for direct mail marketing can often be based on the legitimate interests provision. When direct marketing is based on the legitimate interests provision, the data subject has an absolute right to object: to opt out.[285]

The GDPR has a separate provision that refers to Do Not Track-like systems: in the online context, "the data subject may exercise his or her right to object by automated means using technical specifications."[286] The Do Not Track standard should enable people to signal with their browser that they do not want to be tracked on the internet.[287]

### *6.6 Right to erasure ("to be forgotten")*

The GDPR grants data subjects, under certain circumstances, a right to erasure: "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."[288] The GDPR presents the right

---

[279] Article 21(1) GDPR.
[280] Article 21(6) GDPR.
[281] Article 21(3) GDPR. See also Article 21(2) and Recital 70 GDPR.
[282] "Direct marketing in the on-line environment refers to one-to-one marketing activities where individuals are targeted," says a code of conduct of the Federation of European Direct and Interactive Marketing. The Working Party approved the code in Article 29 Working Party, 'Opinion 4/2010 on the European Code of Conduct of FEDMA for the Use of Personal Data in Direct Marketing' (WP 174), 13 July 2010.
[283] Article 29 Working Party, 'Opinion 03/2013 on purpose limitation', WP 203, 2 April 2013, p. 46. Moreover, Article 5(3) of the ePrivacy Directive generally requires the internet user's consent before companies may place non-necessary cookies.
[284] Article 6(f) GDPR. See Recital 47 GDPR.
[285] The e-Privacy Directive has a similar regime for commercial email and spam. Article 13 e-Privacy Directive.
[286] Article 21(5) GDPR. See also Recital 59 GDPR.
[287] See generally on Do Not Track and European law: F.J. Zuiderveen Borgesius, J. Van Hoboken, K. Irion, and M. Rozendaal, *An Assessment of the Commission's Proposal on Privacy and Electronic Communications*, Directorate-General for Internal Policies, Policy Department C: Citizen's Richts and Constitutional Affairs, June 2017, https://ssrn.com/abstract=2982290
[288] Article 17(1) GDPR.

to erase data as the "right to erasure ('right to be forgotten')."[289] The phrase "right to be forgotten" was not used in the Directive. In summary, a data subject has a right to erasure when the data subject successfully exercises the right to object, when the personal data were unlawfully processed, should be erased because of a legal obligation, or are no longer necessary in relation to the processing purposes.

The right to erasure also applies when the processing is based on the data subject's consent, and the data subject withdraws consent. And the right applies if the data are processed on the basis of the consent of a data subject younger than 16. The preamble says that the erasure right is especially relevant "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."[290] An example could be an old profile on a social networking site that somebody made when young, including embarrassing pictures. He or she might want to have the profile deleted. In many cases, personal data will be spread from the original source all over the internet. Therefore, the GDPR requires the controller to make a reasonable effort to erase the personal data elsewhere on the internet, taking account of available technology and the costs of implementation.[291]

The right to erasure does not apply when erasure conflicts with the freedom of expression.[292] This provision aims to balance freedom of expression and data protection rights. Striking this balance is notoriously difficult. The Court of Justice of the European Union decided in its Google Spain judgment that data subjects in Europe have, under certain conditions, the right to have search results for their name delisted from the search results.[293]

The GDPR gives an additional list of exceptions to the right to erasure. In summary, the right to erasure does not apply if the data processing is necessary because of a legal obligation, for reasons of public interest in the area of public health, for certain archiving or statistical purposes, and for exercising legal claims.[294]

### *6.7 Rights regarding automated decision-making*

Finally, the GDPR contains a provision on the rights of data subjects when they are being profiled or subjected to computerized decision-making processes.[295] The GDPR introduces a definition of profiling: "any form of automated processing of personal data

---

[289] Article 17 GDPR.
[290] Recital 65 GDPR. See also Recital 66 GDPR.
[291] Article 17(2) GDPR.
[292] Article 17(3)(a) GDPR.
[293] CJEU, Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González', Case C-131/12, 2014. See also: S. Kulk and F.J. Zuiderveen Borgesius, *Privacy, Freedom of Expression, and the Right to Be Forgotten in Europe* (draft chapter, February 25, 2017). Cambridge Handbook of Consumer Privacy, eds. Jules Polonetsky, Omer Tene, and Evan Selinger (Cambridge University Press, 2017). https://ssrn.com/abstract=2923722
[294] Article 17(3) GDPR.
[295] Article 22 GDPR. The provision is based on Article 15 of the Directive, which was inspired by French law. See on that old provision: L. A. Bygrave, *Minding the Machine: Article 15 of the EC Data Protection Directive and Automated Profiling*, 17 Computer Law & Security Report 17, 2001.

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."[296] This definition covers, for example, behavioral advertising and credit scoring.[297] The GDPR specifies that data subjects should not be subjected to fully automated decisions which produce legal effects or similarly significantly affect him or her.[298] The provision says that a person has "the right not to be subject to" certain decisions. But many scholars assume that this right implies a prohibition (with exceptions) of such decisions.[299]

The GDPR gives three exceptions to this prohibition. In brief, an automated decision can be taken if it is (a) necessary for a contract between the data subject and the data controller; (b) is authorized by a law which includes suitable safeguards for the data subject's interests; or (c) is based on the data subject's explicit consent.[300] In situation (a) (contract) and (c) (consent), the data controller must implement suitable measures to safeguard the data subject's 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. Exception (c) is new in the GDPR.

The provision can apply, for instance, if an insurance company uses software to decide whether it offers people an insurance contract. The provision allows such an automated decision if the decision leads to offering somebody a contract, because the person's request to enter into a contract has been met. Companies are also allowed to automatically refuse to enter into a contract with somebody if there are suitable measures to safeguard his or her legitimate interests, such as arrangements to ask for human evaluation. Hence, a company that uses software to automatically deny somebody an insurance contract could, for instance, include a phone number on the website, where people can ask a human to reconsider the automated decision to deny the insurance contract.

In practice, many companies might use profiling, for instance for credit scoring, as an aid for humans that make decisions. Such decisions are mostly outside the scope of the provision on fully automated decisions. The GDPR's provision only applies to a "decision based *solely* on automated processing."[301] The predecessor of the GDPR's automated decision provision has not been applied much in practice; it has remained a

---

[296] Article 4(4) GDPR.
[297] See Recitals 24 and 71 GDPR.
[298] Article 22(1) GDPR.
[299] See e.g. Korff D, *Comments on Selected Topics in the Draft EU Data Protection Regulation* (17 September 2012) http://ssrn.com/abstract=2150145; De Hert P and Gutwirth S, *Regulating profiling in a democratic constitutional state*, in Hildebrandt M and Gutwirth S (eds), *Profiling the European Citizen* (Springer 2008); Sandra Wachter, Brent Mittelstadt & Luciano Floridi, *Why a Right to Explanation of Automated Decision-Making does Not Exist in the General Data Protection Regulation,* International Data Privacy Law (2017); Zuiderveen Borgesius, F. J. (2015) Improving privacy Protection in the Area of Behavioural Targeting. Kluwer law International, p. 283-293.
[300] Article 22(2) GDPR.
[301] Article 22(1) GDPR. The Article 29 Working Party interprets this phrase more generously for the data subject. Article 29 Working Party, 'Guidelines on Automated individual decision-making and profiling for the purposes of Regulation 2016/679' (WP251rev.01), 6 February 2018.

"dead letter."[302] It seems plausible that the GDPR's provision will not be applied much in practice either.[303]

A new requirement in the GDPR is that automated decisions should not be based on special data categories (subject to exceptions).[304] Many scholars warn that profiling and automated decisions can have discriminatory effects.[305] Presumably the aim of preventing unfair discrimination is one of the rationales for the prohibition of profiling measures based on special categories of data. However, it is unclear to what extent this prohibition applies when an automated decision is based on non-special personal data (such as a zip code) that function as a proxy for special categories of data (such as race or skin color).

Also new is that, according to the preamble, the controller must "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."[306]

Additionally, the data subject has the right to learn whether such automated decisions are being made. Under certain circumstances, the data subject has the right to obtain "meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject."[307] New in the GDPR is an explicit requirement for controllers using profiling to minimize the risk of errors. The preamble states that "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."[308]

In conclusion, regarding data subject's rights, the GDPR follows broadly the same logic as the Directive. But the GDPR introduces new rights (to restrict processing and to data portability). Compared with the Directive, the GDPR gives more detail regarding the data subject's rights.

As discussed in section 4, the rules on the legitimacy of data processing and the transfer of personal data have remained largely the same. As discussed in section 3, the rules on the applicability of the EU data protection regime have broadened somewhat. The rights of data subjects, discussed in section 6, largely correspond to the rights in the Data

---

[302] Korff D, *Comments on Selected Topics in the Draft EU Data Protection Regulation* (17 September 2012) http://ssrn.com/abstract=2150145.
[303] See Isak Mendoza & Lee A. Bygrave, *The Right Not to be Subject to Automated Decisions Based on Profiling* (2017) https://ssrn.com/abstract=2964855.
[304] Article 22(4) GDPR.
[305] See e.g. Solon Barocas & Andrew D. Selbst, *Big Data's Disparate Impact,* 104 Calif. Law Rev. 671 (2016); B. Custers, T. Calders, B. Schermer, and T. Zarsky, *Discrimination and privacy in the information society: data mining and profiling in large databases* (Springer 2013).
[306] Recital 71 GDPR.
[307] Article 12(2)(f) GDPR.
[308] Recital 71 GDPR.

Protection Directive. Although the right to be forgotten and the right to data portability are new, there are so many restrictions in the GDPR and so many open ends, that it is far from clear that these new rights will prove to be revolutionary.

The aim of the GDPR is primarily to close the gap between the legal principles and practice. This is achieved through, first, laying down additional obligations for data controllers. As discussed in section 5, the GDPR invests heavily in rules on transparency, technical measures, data protection officers, and Data Protection Impact Assessments. These obligations try to ensure that data controllers implement and execute the various data protection principles. But the main new feature of the GDPR may be that the GDPR takes enforcement much more seriously than the Directive. Enforcement is discussed in the next section.

## 7. ENFORCEMENT

The main reason for adopting a new regulation, replacing the Directive from 1995, was not to introduce new principles or standards. Instead, the GDPR invests heavily in compliance and enforcement. First, the tasks and powers of Data Protection Authorities have expanded considerably. Second, there is a push for further cooperation between EU Data Protection Authorities. Third, there are specific rules for remedies and sanctions when data controllers don't abide by the data protection principles contained in the GDPR. Fourth, the European Commission and an advisory board have been granted powers for standard setting. We discuss each point below.

### *7.1 Tasks and powers of Data Protection Authorities*

The Data Protection Directive specified that supervisory authorities have powers on three levels in particular. First, investigative powers, such as powers of access to data forming the subject-matter of processing operations and powers to collect all the information necessary for the performance of its supervisory duties. Second, powers of intervention, such as delivering opinions before processing operations are carried out, ordering the blocking, erasure, or destruction of data, and imposing a temporary or definitive ban on processing. Third, the power to engage in legal proceedings or to bring these violations to the attention of the judicial authorities; decisions by the supervisory authority which give rise to complaints may be appealed through the courts.[309]

The Directive stressed that each supervisory authority shall hear claims lodged by any person, or by an association representing that person. The Directive also stated that Member States shall provide that the members and staff of the supervisory authority, even after their employment has ended, are to be subject to a duty of professional secrecy with regard to confidential information to which they have access.[310]

The position of Data Protection Authorities has been a matter of controversy, mainly on two points. First, the supervisory authorities are generally underequipped and

[309] Article 28 (3) DPD.
[310] Article 28 (7) DPD.

understaffed and their independence is not always guaranteed. Second, the powers and capacities granted to Data Protection Authorities in national law differ to a large extent; moreover, Data Protection Authorities have often asked for more and wider powers.

Regarding the independence of Data Protection Authorities, the Court of Justice of the European Union has held Member States in violation of the Directive a number of times. For example, when Hungary appointed a Data Protection Supervisor for a six year term, but prematurely brought this term to an end, the Court of Justice of the European Union concluded that this was in violation of the Data Protection Directive's requirement of independence.[311] When Germany, consisting of a number of states, each having their own supervisory authority, subjected these authorities to state scrutiny, the Court of Justice ruled that Germany had incorrectly transposed the requirement that those authorities should be able to perform their functions "with complete independence".[312] A violation was also established when Austria laid down in national law that the managing member of the Data Protection Authority was a federal official subject to supervision, that the office of the Data Protection Authority should be integrated with the departments of the Federal Chancellery, and the Federal Chancellor had an unconditional right to information covering all aspects of the work of the Data Protection Authority.[313] Moreover, even in countries where the independence is formally guaranteed by law, Data Protection Authorities are dependent on the state for their budget, which could make them vulnerable to governmental influence.

The GDPR lays down four elaborate provisions on the position and independence of supervisory authorities.[314] The GDPR states that each Member State shall provide that one or more independent public authorities are responsible for monitoring the application of the GDPR.[315] Each supervisory authority shall act with complete independence in performing the tasks and exercising the powers entrusted to it, the members of the supervisory authority must remain free from external influence, they 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. Each Member State must ensure that the Data Protection 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, and shall ensure that each supervisory authority chooses its own staff which shall be subject to the exclusive direction of the member or members of the supervisory authority. Member States must also ensure that each supervisory authority has separate, public, annual budgets.[316] Furthermore, each member of a Data Protection Authority must be appointed by means of a transparent procedure and a member may only be dismissed in cases of serious

---

[311] CJEU, European Commission, supported by: European Data Protection Supervisor (EDPS) v Hungary, C-288/12, 8 April 2014.
[312] CJEU (Grand Chamber) European Commission, v Federal Republic of Germany, 9 March 2010, Case C-518/07.
[313] CJEU (Grand Chamber) European Commission v Republic of Austria, 16 October 2012, Case C-614/10.
[314] Articles 51-54 GDPR. See further Recitals 117-124 GDPR.
[315] Article 51 GDPR.
[316] Article 52 GDPR.

misconduct or if the member no longer fulfils the conditions required for the performance of the duties.[317]

The lack of powers and capacities is also addressed by the GDPR. Many felt that Data Protection Authorities should be better equipped to assess the many data processing initiatives and take measures accordingly, not only through granting them additional financial and administrative means, but also by bestowing more powers and capacities on them. In 2010, the European Commission remarked: "There is consensus among stakeholders that the role of Data Protection Authorities needs to be strengthened so as to ensure better enforcement of data protection rules."[318] This is exactly what the GDPR intends to do. The GDPR grants Data Protection Authorities a wide range of powers and competences, which are listed in the tables below.

| **Tasks**[319] | |
|---|---|
| | |
| monitor and enforce the application of this Regulation | advise on the processing operations |
| promote public awareness of the risks, rules, safeguards and rights in relation to the processing of personal data, especially when children are affected | encourage the drawing up of codes of conduct and give an opinion and approve such codes of conduct which provide sufficient safeguards |
| advise the national parliament, the government, and other institutions on legislative and administrative measures relating to processing personal data | encourage the establishment of data protection certification mechanisms and data protection seals and marks pursuant and approve the criteria of certification |
| promote the awareness of controllers and processors of their obligations | carry out a periodic review of certifications |
| upon request, provide information to any data subject concerning the exercise of their rights | draft and publish the criteria for accreditation of a body for monitoring codes of conduct and of a certification body |
| deal with complaints lodged and investigate the subject matter and inform the complainant of the progress and the outcome of the investigation | conduct the accreditation of a body for monitoring codes of conduct and of a certification body |
| cooperate with, including sharing information and provide mutual assistance to, other supervisory authorities | authorise contractual clauses and provisions |
| conduct investigations on the application of this Regulation, including on the basis | approve binding corporate rules |

[317] Article 52 GDPR. See for the conditions: Article 53 GDPR.
[318] A comprehensive approach on personal data protection in the European Union, Brussels, 4.11.2010 COM(2010) 609 final, p. 4.
[319] Article 57 GDPR.

| | |
|---|---|
| of information received from another supervisory authority | |
| monitor relevant developments, in particular the development of information and communication technologies and commercial practices | contribute to the activities of the European Data Protection Board |
| adopt standard contractual clauses | keep internal records of breaches of this Regulation and of measures taken, in particular warnings issued and sanctions imposed |
| establish and maintain a list in relation to the requirement for data protection impact assessment | fulfil any other tasks related to the protection of personal data |

| **Powers**[320] | | |
|---|---|---|
| **Investigatory powers** | **Corrective powers** | **Authorization and advisory powers** |
| | | |
| order the controller and the processor to provide any information it requires | issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of this Regulation | advise the controller in accordance with the prior consultation procedure |
| carry out investigations in the form of data protection audits | issue reprimands to a controller or a processor where processing operations have infringed provisions of this Regulation; | issue, on its own initiative or on request, opinions to the national parliament, the government or to other institutions and to the public on any data protection related issue |
| carry out a review on certifications issued | order the controller or processor to comply with the data subject's requests to exercise his rights | authorize processing, if the law of the Member State requires such prior authorization |
| notify the controller or the processor of an alleged infringement of this Regulation | order the controller or processor to bring processing operations into compliance with the GDPR | issue an opinion and approve draft codes of conduct |
| obtain, from the controller and the processor, access to all personal data and information necessary | order the controller to communicate a personal data breach to the data subject | accredit certification bodies |

[320] Article 58 GDPR.

| | | |
|---|---|---|
| obtain access to any premises of the controller and the processor, including to any data processing equipment and means | impose a temporary or definitive limitation including a ban on processing | issue certifications and approve criteria of certification |
| | order the rectification, restriction or erasure of data and the notification of such actions to recipients to whom the data have been disclosed | adopt standard data protection clauses |
| | withdraw a certification or to order the certification body to withdraw a certification issued or to order the certification body not to issue certification if the requirements are not or no longer met | authorize contractual clauses |
| | impose an administrative fine | authorize administrative agreements |
| | order the suspension of data flows to a recipient in a third country or international organization. | approve binding corporate rules |

### *7.2 Lead supervisory authority*

With regard to the rules and enforcement thereof within the EU, the Directive laid down rules that EU Member States had to implement and adopt in their national legislation. Consequently, different standards and levels of data protection exist within the European Union. Moreover, as discussed above, the powers and capacities of the different Data Protection Authorities to enforce those rules differ to an even greater extent. Therefore, many companies chose to locate their European headquarters in countries with a low regulatory burden or with underequipped Data Protection Authorities. The Data Protection Directive only contained marginal rules on the cooperation between the different Data Protection Authorities, as it specified that each supervisory authority is competent to exercise, on the territory of its own Member State, the powers conferred on it, but that the supervisory authorities shall cooperate with one another to the extent necessary for the performance of their duties.[321]

[321] Article 28 Data Protection Directive.

In 2015, the European Court of Justice made clear that a Data Protection Authority can exercise its powers of intervention only within the territory of its own Member State. Accordingly, a Data Protection Authority who is not established in the territory concerned cannot impose sanctions on the controller with respect to the processing of data, but should instead request the supervisory authority within the Member State whose law is applicable to act.[322] The problem with this disparity between the rules and the enforcement thereof in Europe is not only that companies can circumvent strict rules by placing their headquarters in Ireland, but also that companies operating in different EU countries are faced with many different duties and obligations. The European Commission noted in 2012: "Heavy criticism has been expressed regarding the current fragmentation of personal data protection in the Union, in particular by economic stakeholders who asked for increased legal certainty and harmonisation of the rules on the protection of personal data."[323]

The GDPR aims to harmonize both the regulation and enforcement of data protection within the European Union. First, a regulation, as opposed to a directive, has direct effect throughout the European Union. Second, the sanctions, fines, and administrative measures are laid down in detail in the GDPR (discussed in the next section). Third, the GDPR contains detailed rules on the cooperation between the different national Data Protection Authorities on the matter of the enforcement of the data protection principles.

The GDPR introduces the concept of "lead supervisory authority".[324] The supervisory authority of the "main establishment" of the controller or processor shall be competent to act as lead supervisory authority for the cross-border processing of this controller or processor.[325] The "main establishment" is the place of a controller's central administration, or the place where the decisions on the purposes and means of the processing of personal data are taken.[326] With respect to the processor, the main establishment is the establishment with its central administration, or the establishment where the main processing activities in the context of the activities of an establishment of the processor take place.[327]

The lead supervisory authority shall cooperate with the other concerned supervisory authorities to reach consensus, except in the case of an emergency.[328] The lead supervisory authority and the concerned supervisory authorities shall exchange all relevant information with each other, and the lead supervisory authority may request at any time that other concerned supervisory authorities provide mutual assistance and may conduct joint operations.[329] The GDPR also contains rules on mutual assistance

---

[322] CJEU, Weltimmo s. r. o. v. Nemzeti Adatvédelmi és Információszabadság Hatóság, C-230/14, 1 October 2015.
[323] Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) /* COM/2012/011 final - 2012/0011 (COD), p. 4.
[324] Recitals 125-128 GDPR.
[325] Article 56 GDPR.
[326] Article 4(16) GDPR.
[327] See further: Recital 36 GDPR.
[328] Article 66 GDPR.
[329] Article 60 GDPR.

between the Data Protection Authorities. The GDPR specifies that the supervisory authorities shall provide each other with relevant information and mutual assistance in order to implement and apply the GDPR 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 authorizations and consultations, inspections, and investigations.[330] Finally, the GDPR specifies that the supervisory authorities shall, where appropriate, conduct joint operations, including joint investigations and joint enforcement measures, in which members or staff from other Member States' supervisory authorities are involved.[331]

### *7.3 Remedies, liabilities, and sanctions*

Throughout the existence of data protection instruments in Europe, one problem has been the lack of effective sanctions and the low fines for data controllers violating the data protection principles. The Data Protection Directive left it mostly to the individual Member States to provide for rules on remedies, liability, and sanctions. On the matter of remedies, the Directive merely specified that Member States had to grant people the right to a judicial remedy for any breach of their rights.[332] Regarding liability, the Directive stated that Member States must provide that any person who has suffered damage as a result of an unlawful processing operation is entitled to receive compensation from the controller for the damage suffered.[333] In relation to sanctions, the Directive specified that Member States must adopt suitable measures to ensure the full implementation of the provisions of the Directive and lay down the sanctions in case of infringement of the provisions adopted pursuant to the Directive.[334]

However, some countries adopted rules allowing for maximum fines or penalties of a couple of thousand euros. It has been broadly recognized that these amounts are insufficient to influence larger internet companies with revenues of millions of euros or dollars per year. For example, in 2010, the European Commission held: "to ensure the enforcement of data protection rules, it is essential to have effective provisions on remedies and sanctions."[335]

The GDPR brings about a change on three points: remedies, liability, and sanctions. The changes with respect to sanctions are the most spectacular.[336] With regard to the right to compensation and liability, the GDPR has little new. Regarding the remedies, the GDPR specifies that every data subject shall have the right to lodge a complaint with a supervisory authority.[337] Natural or legal persons shall also have the right to an effective judicial remedy against a legally binding decision of a supervisory authority

---

[330] Article 61 GDPR.
[331] Article 62 GDPR.
[332] Article 22 Data Protection Directive.
[333] Article 23 Data Protection Directive.
[334] Article 24 Data Protection Directive.
[335] A comprehensive approach on personal data protection in the European Union, Brussels, 4.11.2010 COM(2010) 609 final, p. 9.
[336] See also: Recitals 129-138 GDPR.
[337] Article 77 GDPR.

concerning them.[338] Furthermore, the GDPR specifies that each data subject has the right to an effective judicial remedy if they consider that their rights have been infringed as a result of the processing of their personal data. Proceedings against a controller or processor shall be brought before the courts of the Member State where the controller or processor has an establishment.[339] The possibility of representation is further elaborated on in the GDPR, as the data subject is often incapable of engaging in long and costly legal proceedings against governmental organizations or multinationals with fully equipped and resourced legal teams. The GDPR holds that the data subject shall have the right to mandate a body, organization, or association, which is of non-profit making character, and whose statutory objectives are in the public interest, to lodge the complaint on his or her behalf.[340]

There is a significant change regarding administrative fines. The GDPR distinguishes two situations. First, there is the possibility of imposing administrative fines up to ten million euro or, in the case of an undertaking, up to 2% of the total worldwide annual "turnover" (not "profit") of the preceding financial year, whichever is higher. Such fines may be imposed if the data controller violates the rules on, inter alia, the conditions for consent given by children, data protection by design and by default, the division of responsibilities between different controllers and processors, the keeping of documents and records on the data processing activities, the obligation to provide a notification to either the Data Protection Authority or the data subject in case of a data breach, and carrying out a Data Protection Impact Assessment.[341]

Second, there is the possibility of an administrative fine of up to 20 million euro or, in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher. Such fines can be imposed, inter alia, in case of a violation of the data minimization principle, the purpose limitation principle, the accuracy principle, the integrity and confidentiality principle, the rights of data subjects (such as the right to be informed and the right to correct or erase data), the transparency obligations, and the rules on trans-border data flows.[342]

### *7.4 European Data Protection Board and the European Commission*

The Directive held that there should be a Working Party. That Working Party is commonly known as the Article 29 Working Party, because it is established through Article 29 of the Data Protection Directive. The Working Party has several tasks. The Working Party can, on its own initiative, make recommendations on all matters relating to the protection of persons with regard to the processing of personal data in the Community.[343] Since the introduction of the Data Protection Directive, the Working Party has published more than two hundred opinions and recommendations on the

---

[338] Article 78 GDPR.
[339] Article 79 GDPR.
[340] Article 80 GDPR.
[341] Article 83(3) GDPR.
[342] Article 83(4) GDPR.
[343] Article 30 Data Protection Directive.

application and interpretation of the data protection principles. Although the Working Party's opinions are generally seen as authoritative, they have no formal legal status.[344]

The general feeling was that the institutional protection of data protection should not only be strengthened on a national level, by expanding the powers and capacities of Data Protection Authorities, but also on a European level. Among others, the European Commission noted that in respect of the enforcement of the data protection principles, "the continuing divergent application and interpretation of EU rules by Data Protection Authorities, (…) calls for a strengthening of the Working Party's role in coordinating Data Protection Authorities' positions, ensuring a more uniform application at national level and thus an equivalent level of data protection."[345]

Indeed, the powers and capacities of the Working Party are expanded in the GDPR. To emphasize the changes, the Article 29 Working Party has been renamed the European Data Protection Board.[346] One of the core functions of the European Data Protection Board is guiding the process of cooperation between different national Data Protection Authorities. The GDPR specifies, among others, that the European Data Protection Board shall issue an opinion whenever a competent supervisory authority intends to adopt a list of the processing operations subject to the requirement for a Data Protection Impact Assessment, aims to authorize contractual clauses, aims to approve binding corporate rules, aims to approve the criteria for accreditation of a body, etc.[347] The European Data Protection Board shall adopt a binding decision, inter alia, where a supervisory authority concerned has expressed a relevant and reasoned objection to a draft decision of the lead authority and where there are conflicting views on which of the supervisory authorities concerned is competent for the main establishment.[348]

The GDPR also specifies that the European Data Protection Board shall be composed of the head of one supervisory authority of each Member State and of the European Data Protection Supervisor.[349] The GDPR emphasizes the independence of the European Data Protection Board by specifying that it shall act independently and without prejudice to requests by the European Commission.[350] The European Data Protection Board shall draw up an annual report regarding the protection of natural persons with regard to the processing of personal data in the Union and, where relevant, in third countries and international organizations.[351] What is most important, however, is the increase in tasks and powers of the European Data Protection Board, as shown in the table below.

---

[344] See generally on the Working Party: Gutwirth S and Poullet Y, The contribution of the Article 29 Working Party to the construction of a harmonised European data protection system: an illustration of "reflexive governance"? in Asinari VP and Palazzi P (eds), *Défis du Droit à la Protection de la Vie Privée. Challenges of Privacy and Data Protection Law* (Bruylant 2008).
[345] A comprehensive approach on personal data protection in the European Union, Brussels, 4.11.2010 COM(2010) 609 final, p. 17-18.
[346] See on its functioning also: Recitals 139-143 GDPR.
[347] Article 64 GDPR.
[348] Article 65 GDPR.
[349] Article 68 GDPR.
[350] Article 69 GDPR.
[351] Article 71 GDPR. See further recitals 72 and 77 GDPR.

| **Tasks of the European Data Protection Board** [352] | |
|---|---|
| | |
| monitor and ensure the correct application of the GDPR | encourage the drawing-up of codes of conduct and the establishment of data protection certification mechanisms and data protection seals and marks |
| advise the Commission on any issue related to the protection of personal data in the Union | carry out the accreditation of certification bodies and its periodic review and maintain a public register of accredited bodies and of the accredited controllers or processors established in third countries |
| advise the Commission on the format and procedures for the exchange of information between controllers, processors and Data Protection Authorities for binding corporate rules | specify the requirements with a view to the accreditation of certification bodies |
| issue guidelines, recommendations, and best practices on procedures for deleting links, copies or replications of personal data (right to be forgotten) | advise the Commission on the certification requirements |
| examine any question covering the application of the GDPR and issue guidelines, recommendations and best practices to encourage consistent application | advise the Commission on the icons |
| issue guidelines, recommendations and best practices for further specifying the criteria and conditions for decisions based on profiling | advise the Commission on the assessment of the adequacy of the level of protection in a third country or international organization |
| issue guidelines, recommendations and best practices for establishing data breaches and for the circumstances for notifying such breaches | issue opinions on draft decisions of supervisory authorities pursuant to the consistency mechanism |
| issue guidelines, recommendations and best practices as to the circumstances in which a personal data breach is likely to result in a high risk | promote the cooperation and the effective bilateral and multilateral exchange of information and practices between the supervisory authorities |
| issue guidelines, recommendations and best practices to specify the criteria and requirements for data transfers based on binding corporate rules | promote common training programmes and facilitate personnel exchanges between the supervisory authorities |

[352] Article 70 GDPR.

| | |
|---|---|
| issue guidelines, recommendations and best practices to specify the criteria and requirements for the data transfers | promote the exchange of knowledge and documentation on data protection legislation and practice with Data Protection Authorities worldwide. |
| draw up guidelines for supervisory authorities concerning the application of measures and the fixing of administrative fines | issue opinions on codes of conduct drawn up at Union level |
| review the practical application of the guidelines, recommendations and best practices | maintain a publicly accessible electronic register of decisions taken by supervisory authorities and courts on issues dealt with in the consistency mechanism |
| issue guidelines, recommendations and best practices for establishing common procedures for reporting by individuals of infringements | |

The role of the European Commission was limited in the Directive. Its main competence was to declare that third countries had an adequate level of protection.[353] As noted, this competence is maintained in the GDPR, but the Commission's powers and capacities have been broadened significantly.[354] The power to adopt delegated acts is conferred on the Commission in two instances.[355] First, the Commission is empowered to adopt delegated acts to determine the information to be presented by and the procedures for providing standardized icons. Second, the Commission is empowered to adopt delegated acts to specify the requirements to be taken into account for the data protection certification mechanisms. Furthermore, the Commission may adopted regulation and delegated acts on a number of provisions under the GDPR. Finally, Member States, the Data Protection Authorities and the European Data Protection Board have a general obligation to fully inform the Commission of all actions and decisions they take.

## 8. CONCLUSION

This paper discusses the new General Data Protection Regulation (GDPR) of the European Union, which enters into force in 2018. The GDPR will replace the 1995 Data Protection Directive, one of the world's most influential data privacy texts. The core of data protection law proves to be remarkably stable. Data protection's core principles, comparable to the Fair Information Principles, are retained in the GDPR.

However, the GDPR also brings significant changes. For instance, unlike a directive, a regulation does not have to be implemented in the national laws of the EU Member States. The GDPR should thus lead to a more harmonized regime in Europe. The most

[353] See further Article 31 Data Protection Directive.
[354] See similar to Article 31 Data Protection Directive, Article 92-93 GDPR.
[355] Article 92 GDPR.

important change is probably the strengthening of enforcement possibilities. Data Protection Authorities can impose fines for non-compliance of up to 4% of the worldwide turnover of companies.

The GDPR is the world's strictest and most comprehensive data privacy law, and it is a well-meaning and ambitious piece of legislation. The main disadvantage of the GDPR is its length and complexity: 99 detailed provisions. Whether the GDPR will actually improve fairness and respect for fundamental rights can, of course, only be assessed when it has been applicable for some time.

EU Member States now have to fill in the blanks where the GDPR gives them the possibility, and sometimes a requirement, to do so. As the GDPR gives Member States room for maneuver, it seems unlikely that the GDPR will lead to a completely harmonized regime in the EU. For instance, Member States must reconcile the GDPR with the right to freedom of expression and information. Different Member States take different approaches to balancing freedom of expression on the one hand, and privacy and data protection on the other.

Meanwhile, the European Commission has started its next data privacy project. The Commission has published a proposal for an ePrivacy Regulation,[356] which should replace the ePrivacy Directive. The proposal includes rules to protect confidentiality of communications on the internet, and rules regarding cookies and online tracking.

The rules for fair processing of personal data will never be finished. Just like in consumer protection law or environmental law, the rules will have to be updated and amended continually, to adapt to new circumstances. In conclusion, the GDPR signals a new phase in data privacy law, and will influence policy worldwide.

* * *

[356] See F.J. Zuiderveen Borgesius, J. Van Hoboken, K. Irion, and M. Rozendaal, An Assessment of the Commission's Proposal on Privacy and Electronic Communications, Directorate-General for Internal Policies, Policy Department C: Citizen's Rights and Constitutional Affairs, June 2017, https://ssrn.com/abstract=2982290.