Hastings Science and Technology Law Journal

Volume 11
Number 2 *Summer 2020*

Article 2

Summer 2020

Binding Effects of the European General Data Protection Regulation (GDPR) on U.S. Companies

Manuel Klar

Binding Effects of the European General Data Protection Regulation (GDPR) on U.S. Companies

DR. MANUEL KLAR*

Table of Contents

I. INTRODUCTION 102
II. DIRECT APPLICABILITY OF THE GDPR 105
A. Territorial Scope 105
B. Material Scope 126
III. APPLICABILITY OF NATIONAL DATA PROTECTION LAW OF THE EU MEMBER STATES 133
IV. CONTRACTUAL SUBJECTION TO THE RULES OF THE GDPR 135
A. Agreement on Commissioned Data Processing 136
B. Joint Controllership Agreement 138
C. StandardContractual Clauses of the European Commission 140
V. CONSEQUENCES FOR U.S. COMPANIES WHICH ARE SUBJECT TO THE GDPR 141
A. Appointment of a Representative in the EU 142
B. Further Duties 143
VI. CONCLUSION 153

* Attorney in the law firm of Gleiss Lutz in Munich, Germany and lecturer on data protection law at the University of Regensburg. In the spring of 2015 the author deepened his knowledge of data protection law in the course of a comparative law research project at the University of California, Berkeley. The author thanks Robin Leick for his valuable assistance in the preparation of this manuscript.

I. Introduction

The territorial scope of the European General Data Protection Regulation (GDPR), which has been in force since May 25, 2018,[1] extends well beyond the European borders. In the past, European data protection law had already applied for companies which had an establishment in the European Union (EU). Now under the GDPR, the territorial scope has expanded through the introduction of a "marketplace rule" or "destination approach."[2] As a result, the new provisions of European data protection law also apply for the first time to companies worldwide which are not domiciled in the European Union, but offer goods or services to data subjects in the European Union or monitor their behavior. As this examination will show, the hurdles for the geographic applicability of the GDPR are by no means high. As a matter of fact, a great many companies outside of the EU have to comply with European data protection law. This affects not only large international corporate groups, but also small and medium-sized companies in particular.[3] The new stipulations on the GDPR's extraterritorial effect are therefore considered, not without reason, the most significant regulations therein.[4]

Along with the new provisions on the territorial scope, it is also worth taking a closer look at the provisions of the GDPR on its material scope, which forms the second pillar of the applicability of the GDPR. In particular, the key concept of European data protection law, namely "personal data", is interpreted much more broadly in a European context than under U.S. law. One example of this would be IP addresses which, according to a judgment of the European Court of Justice (ECJ), could fall under the scope of the

1. Regulation (EU) 2016/679 of the European Parliament and 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), 2016 O.J. K 119/1.

2. Adèle Azzi, *The Challenges Faced by the Extraterritorial Scope of the General Data Protection Regulation*, 9 JIPITEC 126, 129 (2018); Paul de Hert & Michal Czerniawski, *Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context*, 5 IDPL 230, 231 (2015).

3. Craig McAllister, *What about small businesses? The GDPR and its consequences for small, U.S.-based companies*, 12 BROOK. J. CORP. FIN. & COM. L. 187, 192 (2018).

4. Dan Jerker B. Svantesson, *The Extraterritoriality of EU Data Privacy Law – Its Theoretical Justification and Its Practical Effect on U.S. Businesses*, 50 STAN. J. INT'L. L. 53, 71 (2014): "For any non-EU party, Article 3 is the single most important provision in the entire proposed Regulation […]"; Anna Zeiter, *The New General Data Protection Regulation of the EU and its Impact on IT Companies in the U.S.*, 20 TTLF Working Paper 1, 9 (2014).

GDPR as personal data.[5] In this regard as well, it can therefore be advisable for U.S. companies to examine the European legal situation.

And even if the provisions of the GDPR are not directly applicable for U.S. companies, EU companies which exchange personal data with U.S. companies often have to obligate them contractually to maintain a data protection standard similar to that of the GDPR. This is especially the case if the data exchange falls under the category of "commissioned data processing" or "joint controllership" in the sense of the GDPR and/or the data transfer to the United States is to be secured by way of the standard contractual clauses of the European Commission. In its recent rulings on *Facebook Fanpages* and *Fashion ID*,[6] the ECJ laid the foundation for a broad interpretation of the GDPR's stipulations on joint controllership with regard to tracking services on the internet which is likely to have far-reaching consequences for the cookie and tracking industry. This also comes down to an indirect "export" of European data protection standards.

It is therefore to be expected that the expansive effect of the stringent European data protection rules, which had been initiated previously by European Directive 95/46/EC[7, 8] will continue to grow in the future.[9] The intention of the European legislature here is clear. Companies outside of the EU which, like European companies, are economically active on the European market, are now also to be caught in the crosshairs of data

5. For more on this, *see* II.B.2. below.

6. ECJ Case C-210/16, Facebook Fanpages, 2018 ECLI:EU:C:2018:388, (*available at* http://curia.europa.eu/juris/document/document.jsf?docid=202543&text=&dir=&doclang=EN&part=1&occ=first&mode=lst&pageIndex=0&cid=1442187); Case C-40/17, Fashion ID, 2019 ECLI:EU:C:2019:629, (*available at* http://curia.europa.eu/juris/document/document.jsf;jsessionid=35B2D4A969007395F748FAA31C02C3DC?text=&docid=216555&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=2128539); *see also* ECJ Case C-25/17, Jehovah's Witnesses, 2018 ECLI:EU:C:2018:551, (*available at* http://curia.europa.eu/juris/document/document.jsf?text=&docid=203822&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=2129026).

7. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 1995 O.J. L. 281/31 (hereinafter European Directive 95/46/EC).

8. On the inclusion of the extraterritorial approach of Article 4 of Directive 95/46/EC in the data protection laws of other states, see Svantesson, *supra* note 4, at 89; restrictively, Kurt Wimmer, *Free Expression and EU Privacy Regulation: Can the GDPR Reach U.S. Publishers?* 68 SYRACUSE L. REV. 547, 563 (2018).

9. *See* Merlin Gömann, *The new territorial scope of EU data protection law: deconstructing a revolutionary achievement*, 45 CML REV. 567, 568 (2017); critical: Dan Jerker B. Svantesson, *European Union Claims of Jurisdiction over the Internet – an Analysis of Three Recent Key Developments*, 9 JIPITEC 113 para. 28 (2018); critical from an international law perspective: Azzi, *supra* note 2, at 130; Wimmer, *supra* note 8, at 557.

protection law. In light of this expansion of the scope and, related to this, the definition of who is subject to European data protection law, more and more companies outside of the EU will also need to concern themselves with European data protection requirements in the future. This is particularly the case for companies in the US, since that is where such key digital economy players as Google, Facebook, YouTube and WhatsApp in fact come from. Impressive evidence of this was provided by the Google case, in which the French data protection authority CNIL imposed a fine of EUR 50 million on Google LLC at the beginning of 2019.[10] This can also serve as a paradigm for a new era in the enforcement of European data protection rules. However, the applicability of the GDPR is by no means limited to the global players in the IT sector. Even the simple placement of tracking cookies on websites of U.S. companies which can be accessed by citizens in the EU can, under certain circumstances, lead to the applicability of the GDPR and as a result to an obligation to comply with the extremely lengthy list of requirements it imposes on so-called data controllers. In the event of a material breach of the requirements of the GDPR, European data protection supervisory authorities may issue remedial orders or impose administrative fines of (theoretically) up to EUR 20 million or 4% (for formal breaches: EUR 10 million or 2%) of the total worldwide annual turnover of the preceding financial year, whichever is higher (see Article 83 GDPR). This could potentially compel U.S. companies to reexamine, and possibly change, their current structures and processes.[11] However, it is still completely unclear whether, and if so how, the European supervisory authorities will actually enforce the requirements under the GDPR on companies outside of the EU.

In the following, I will examine in what situations U.S. companies can be bound by the rules of the GDPR, with an overview of the specific duties they will need to fulfill where it does apply. First of all, the territorial and material scope of the GDPR will be outlined, with a particular focus on the new marketplace rule (Section II). This will be followed by a discussion of the fact that despite its direct applicability and binding effect in the Member States of the European Union, the GDPR does also grant the Member States a great deal of national leeway for enacting special data protection rules (Section III). I will then examine classic types and contents of data protection contracts which EU companies may be obligated to conclude under the GDPR if they exchange personal data with U.S. companies. This can lead to

10. *See* Commission Nationale de l'Informatique et des Libertés, The CNIL's restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC, 21 January 2019, (*available at* https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penal ty-50-million-euros-against-google-llc).

11. McAllister, *supra* note 3, at 201.

an indirect applicability of European data protection law provisions to U.S. companies in this regard (Section IV). Finally, I will describe the essential obligations that U.S. companies must meet should the GDPR be applicable to them (Section V). A conclusion will round off this article and give a perspective of possible future developments (Section VI).

II. Direct Applicability of the GDPR

The GDPR applies for U.S. companies that fall within both its territorial and its material scope, as regulated in Articles 3 and 2, respectively.[12] These provisions thus essentially "open the door" to the GDPR. The prerequisites for applicability are the subject of the following examination (see A. and B.). The GDPR applies without differentiation to any natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data (the "controller"),[13] or which processes the personal data on behalf of a controller (the "processor").[14] In this connection it is important to note that the applicability of the GDPR cannot be set aside by way of choice of law clauses.

A. Territorial Scope

In the context of Article 3 GDPR, three scenarios can be distinguished in which the territorial scope of the GDPR applies for U.S. companies.[15]

12. Article 3 GDPR: "1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.

2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to: (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or (b) the monitoring of their behavior as far as their behavior takes place within the Union. (…)."

Article 2 GDPR: "1. This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.

2. This Regulation does not apply to the processing of personal data: (…) (c) by a natural person in the course of a purely personal or household activity."

13. *See* Article 4 no. 7 GDPR.

14. Article 4 no. 8 GDPR. For more on the terms "controller" and "processor", including the duties they have to perform under the GDPR, see IV. B.

15. On the territorial scope of the GDPR, *see* Manuel Klar, in DS-GVO/BDSG, Art. 3 DS-GVO (Jürgen Kühling & Benedikt Buchner, 2nd ed. 2018).

Firstly, it applies for the processing of personal data insofar as this is carried out in the context of the activities of an establishment in the European Union (Case 1, see 1. below). Secondly, it applies to the processing of personal data of data subjects who are in the European Union where the processing activities are related to the offering of goods or services to data subjects in the European Union (Case 2, see 2. below). And thirdly, the territorial scope applies if the processing activities are related to the monitoring of the behavior of data subjects in the European Union (Case 3, see 3. below). The extraterritorial effects resulting from the expansion of the territorial scope under the GDPR are not to be underestimated and are worth examining more closely (see 4. below).

1. Case 1: Establishment in the European Union

The GDPR applies in Case 1 if a U.S. company as a controller or processor processes personal data in the context of the activities of an establishment in the European Union (Article 3(1) GDPR). This applies regardless of whether the processing takes place in or outside of the European Union and what the nationality is of the person whose data are being processed. Thus, even a mere processing of the data of U.S. citizens would fall within the scope of the GDPR insofar as it takes place in the context of the activities of a U.S. company in the Union.[16] This essentially corresponds to the legal situation under European Directive 95/46/EC, which was then replaced by the GDPR in May 2018.

A central term in the context of Article 3(1) GDPR is "establishment". An establishment implies the "effective and real" exercise of activity through "stable arrangements".[17] Whether or not such "stable arrangements" exist must be determined on the basis of the actual circumstances. In the view of the ECJ, it is necessary to take a "flexible definition" of the concept of "establishment" which rejects any formalistic interpretations.[18] Thus, the legal form of the arrangements, whether simply a branch or a subsidiary with

16. Making reference to the associated European site disadvantage, see the study of the Directorate-General for internal Policies, (Direction A), *Reforming the Data Protection Package*, 49 (2012).

17. *See* recital 22 of the GDPR.

18. ECJ Case C-230/14, *Weltimmo s.r.o. v. Nemzeti Adatvédelmi és Információszabadság Hatóság*, 2015 ECLI:EU:C:2015:639, at para. 29, (*available at* http://curia.europa.eu/juris/document/document.jsf?text=&docid=168944&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=1443262). *See also* de Hert & Czerniawski, *supra* note 2, at 233; Graça Canto Moniz, *Finally: a coherent framework for the extraterritorial scope of EU data protection law – the end of the linguistic conundrum of Article 3(2) of the GDPR*, 4 UNIO – EU LAW JOURNAL 105, 108 (2018).

a legal personality, is not the determining factor. Even internal departments such as production facilities, bookkeeping or data centers without capacity to conclude contracts can constitute an establishment.[19] In particular, in the ECJ's view, it is not of decisive importance whether the undertaking concerned is entered in the registers of the relevant location.[20] Rather, what is required is a combination of the human and technical resources necessary to perform the activities of the arrangement,[21] as well as a certain degree of stability.[22] The provision of a space is not necessarily required, but a facility which is merely installed on a temporary basis does not meet the definition of stable arrangements. Thus, mobile business premises or trade fair stands which are not repeatedly set up do not comprise stable arrangements. If premises are maintained in the European Union on a permanent basis but no human activities of any kind are performed from them, in general this will likewise be insufficient for the assumption of an establishment.[23] Accordingly, purely technical service bases, servers or letterbox entities as

19. Similar with regard to even individual employees, European Data Protection Board, *Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) – Version 2.1*, 5 (2019). The European Data Protection Board is an institution of the European Union with legal personality (*see* Article 68(1) GDPR). The predecessor of the European Data Protection Board was the Article 29 Data Protection Working Party. The European Data Protection Board's task is to ensure the consistent application of the GDPR in the entire European Union. It is composed of the head of one supervisory authority of each Member State and of the European Data Protection Supervisor.

20. ECJ Case C-230/14, *supra* note 18, at para. 29.

21. *See* ECJ Case 168/84, *Berkholz v. Finanzamt Hamburg-Mitte-Altstadt*, 1985 E.C.R. 2251, at para. 18, (*available at* http://curia.europa.eu/juris/showPdf.jsf?text=&docid=93188&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=1444157).

22. On the legal situation under European Directive 95/46/EC *see* ECJ Case C-230/14, *supra* note 18, at para. 29; ECJ Case C-191/15, *Verein für Konsumenteninformation v. Amazon EU Sàrl*, 2016 ECLI:EU:C:2016:612, at para. 77, (*available at* http://curia.europa.eu/juris/document/document.jsf?text=&docid=182286&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=1445005); *see* on the criterion of the permanence of an establishment also ECJ Case C-221/89, *The Queen v. Secretary of State for Transport, ex parte Factortame Ltd and others*, 1991 E.C.R. I-3905, at para. 20, (*available at* http://curia.europa.eu/juris/showPdf.jsf?text=&docid=96817&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=1445492); GDPR European Data Protection Board, *supra* note 19, at 6.

23. Similarly, on the freedom of establishment under Article 49 of the Treaty of the Functioning of the European Union (TFEU) ECJ Case 168/84, *supra* note 21, at para. 18; Article 29 Data Protection Working Party, *Opinion 8/2010 on applicable law*, WP 179, 11 (2010). The Article 29 Data Protection Working Party was the European Commission's independent advisory group on data protection issues until the GDPR entered into effect. It was replaced by the European Data Protection Board which declared many of the positions taken by the Article 29 Data Protection Working Party to be applicable under the GDPR as well.

such do not comprise stable arrangements.[24] The same applies for websites which can be called up in the European Union.[25] Persons such as business travelers or trade show participants who stay in the EU only temporarily are also not to be deemed to comprise stable arrangements, as a rule.[26] However, in the view of the ECJ, under certain circumstances, the mere presence of a single representative in the European Union can be sufficient for applicability of the GDPR. This is the case if the representative is active in the Member State with a sufficient degree of stability, with the resources necessary for the rendering of the relevant specific services, and in particular carries out effective and real activities there.[27] Naturally, this does not include the representative who might have to be designated by the U.S. company pursuant to Article 27 GDPR.[28]

An additional requirement is an "effective and real" exercise of activity through stable arrangements, for which no stringent criteria is to be applied. Its existence must be ascertained on the basis of an overall view, taking into account the particular nature of the activities performed by the stable arrangements and the services in question.[29] For example, in the past, the ECJ assumed a relevant exercise of activity in a case in which a controller had appointed a representative in a Member State who had negotiated with customers in that Member State on the settlement of unpaid receivables and maintained a bank account for the collection of receivables and a post office box for handing the day-to-day business in the sovereign territory of that Member State.[30] On the other hand, if a U.S. company avails itself of the activities of a processor in the EU which merely processes the personal data for that company according to its instructions, in the view of the European Data Protection Board, that processor would not comprise an establishment of the U.S. company in the Union.[31]

The data processing for the controller must occur "in the context of the activities" of the establishment, which depends decisively on the degree or

24. Klar, *supra* note 15, at para. 46.

25. ECJ Case C-191/15, *supra* note 22, at para. 76; European Data Protection Board, *supra* note 19, at 7; cf. also Moniz, *supra* note 18, at 108; in this regard, however, the applicability of the GDPR can derive from Article 3(2) GDPR.

26. *See* Klar, *supra* note 15, at para. 47.

27. *See* ECJ Case C-230/14, *supra* note 18, at para. 29, 30; European Data Protection Board, *supra* note 19, at 7; *see also* Gömann, *supra* note 9, at 575.

28. But Gömann presumably thinks that it does; Gömann, *supra* note 9, at 575.

29. *See* ECJ Case C-230/14, *supra* note 18, at para. 29; European Data Protection Board, *supra* note 19, at 6.

30. ECJ Case C-230/14, *supra* note 18, at para. 29.

31. European Data Protection Board, *supra* note 19, at 12.

the extent to which it is involved in the activities in the context of which personal data are processed.[32] The establishment must be integrated into the relevant data processing, and its activity must have a certain connection with it.[33] For corporate groups this means that they must examine in detail which group company carries out what activities.[34] The establishment must generally be affiliated with the controller to such an extent that the latter has a certain ability to influence the establishment. In the assessment of the ECJ, the requirement of data processing "in the context of the activities" can be met even by mere advertising or sales establishments.[35] Accordingly, it found in its *Google Spain* decision with respect to search engine operators that the phrase "in the context of the activities" is not to be construed narrowly. A relevant participation by the establishment in the data processing does not necessarily require that the processing of personal data be carried out "by" the establishment concerned itself;[36] rather, it is sufficient if the establishment is merely inextricably linked economically to the actual data processing.[37] These prerequisites would be met if a search engine operator in a Member State forms a branch establishment or subsidiary solely to promote sales and sell advertising spaces with which the service offered by the search engine is to be made profitable, and these activities are directed at the inhabitants of that state.[38] Under these circumstances, the activities of the controller and those of its establishment in the relevant Member State

32. Article 29 Data Protection Working Party, *supra* note 23, at 14; *see also* European Data Protection Board, *supra* note 19, at 6.

33. *See* European Data Protection Board, *supra* note 19, at 6.

34. Article 29 Data Protection Working Party, *supra* note 23, at 14; European Data Protection Board, *supra* note 19, at 8.

35. ECJ Case C-131/12, *Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, 2014 ECLI:EU:C:2014:317, (*available at* http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=1449732); *see also* European Data Protection Board, *supra* note 19, at 8; critical: Gömann, *supra* note 9, at 570; de Hert & Czerniawski, *supra* note 2, at 234.

36. ECJ Case C-131/12, *supra* note 35, at para. 52; ECJ Case C-230/14, *supra* note 18, at para. 35; ECJ Case C-191/15, *supra* note 22, at para. 78; *see also* European Data Protection Board, *supra* note 19, at 7; Gömann, *supra* note 9, at 572 et seq.

37. ECJ Case C-131/12, *supra* note 35, at para. 56; *see also* Moniz, *supra* note 18, at 109.

38. ECJ Case C-131/12, *supra* note 35, at para. 50 et seq.; European Data Protection Board, *supra* note 19, at 8; a similar position had already been taken by Article 29 Data Protection Working Party, *Opinion 1/2008 on data protection issues related to search engines*, WP 148, 10 (2008). It was determined that the national data protection law would be applicable if "a search engine provider establishes an office in a Member State (EEA) that is involved in the selling of targeted advertisements to the inhabitants of that state".

would be deemed to be inextricably linked.[39] The considerations set out in this judgment would most likely also be applicable to other website operators and comparable scenarios outside of the internet.[40] As a consequence, data processing in the context of websites of U.S. companies would, in principle, also fall within the scope of European data protection law insofar as they avail themselves of a stable arrangement in the EU to promote their respective core business (e.g., through the sale of advertising and marketing). This is bound to be the case in more than a few scenarios, in which it is very likely that the applicability of the GDPR would also be triggered pursuant to Article 3(2) GDPR, as will be discussed in more detail below.

2. Case 2: Offer of Goods or Services in the European Union

Additionally, the GDPR applies to the processing of personal data of data subjects who are in the Union, where the processing activities are related to the offering of goods or services to these persons, irrespective of whether a payment of the data subject is required (Article 3(2)(a) GDPR).[41] Since the decisive factor in this scenario is that the European market is being addressed, this form of territorial applicability can also be referred to as the "marketplace rule".

With the requirement that the processing activity must be related to persons who "are in the Union", the regulators made the GDPR's applicability with regard to the respective data subject contingent upon a local connection to the territory of the EU. The GDPR does not provide any explanation of how the term "who are in the Union" is to be understood. In terms of time, it is in particular unclear whether a stay in the European Union needs to be on a permanent basis or can only be temporary. It should be sufficient in this regard if the data subject is residing in the European Union at the time of the (first) data processing activity in question.[42] Article 3(2) GDPR pertains not only to European Union citizens within the meaning of Article 9 of the Treaty on European Union (TEU) who are nationals of a Member State, but to all persons who are in the Union, regardless of their place of residence.[43] Consequently, travelers residing outside of the EU, for example, will be subject to the provision in the same way as employees who

39. ECJ Case C-131/12, *supra* note 35, at para. 56; European Data Protection Board, *supra* note 19, at 8.

40. Also, according to the European Data Protection Board, *supra* note 19, at 8.

41. For more on the mechanism of the provision, *see also* Gömann, *supra* note 9, at 583 et seq.

42. European Data Protection Board, *supra* note 19, at 15.

43. Moniz, *supra* note 18, at 113.

are (temporarily) working in the Union.[44] This follows for one thing from the meaning of the word "are", which does not infer any element of permanence. For another thing, this derives from the fact that the regulators deliberately refrained from using the term "residing", which had previously been in the GDPR drafts of the European Commission, the EU Parliament and the Council.[45] Ultimately, this is consistent given the fact that recitals 2 and 14 of the GDPR stipulate that natural persons are entitled to protection of their personal data whatever their nationality or place of residence.

The term "offer" pertains in particular to where the controller or processor submits a declaration of intent to conclude a contract, as well as data processing which is carried out in the context of a mere request to submit an offer. Whether or not a contact is actually concluded is irrelevant. There is no mandatory requirement for any active involvement on the part of the controller or the processor. Even the merely passive availability of an offer on a website can therefore comprise an offer within the meaning of the provision. Otherwise, no serious demands are to be placed on the existence of an offer. This follows from the wording of the provision, under which the data processing merely needs to be "related to" the offering of goods or services. This covers not only data processing relating to the submission of an offer, but also data processing (of one and the same controller) which is simply pursuing the purpose of submitting an offer.[46] Thus, the provision could also cover data processing which is carried out prior to or following an offer, in particular if it is carried out for advertising purposes, e.g. in connection with the ordering of advertising or informational material from the website of a hotel.

The European Data Protection Board holds that if a company in the U.S. uses a processor from the U.S. or another non-EU/EEA country, then the processor should (in light of the regulations that are applicable for it) be subject to the GDPR if that controller is subject to the GDPR pursuant to Article 3(2) GDPR.[47] However, the applicability of the GDPR would most likely not be triggered for a controller in the U.S. which, although it processes personal data of persons in the Union, has merely obtained them from another controller which, for its part, had collected and processed the data within the scope of an offer of goods or services to persons in the

44. *See also* Moniz, *supra* note 18, at 115.

45. *See, e.g.*, European Commission, 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) 11 final, 41.

46. Also according to the European Data Protection Board, *supra* note 19, at 17.

47. European Data Protection Board, *supra* note 19, at 21.

Union.[48] To that extent, the "chain" of responsibility (which can still be assumed to exist between a controller and a processor in the U.S.) is broken, and the transfer of data to the other controller in the U.S. (which is not subject to the GDPR) needs only be taken into account in the course of ascertaining the lawfulness of the transmission. Taking the view that the other controller in the U.S. would likewise be subject to the GDPR would lead to an unjustifiable difference in valuation compared to a controller in the U.S. which is subject to the GDPR pursuant to Article 3(1) GDPR and would like to transmit the relevant data to another controller in the US, as in that case, the other controller would not fall within the scope of the GDPR. Finally, as it is of no importance how frequently the controller or processor offers goods or services, data processing related to a one-time or first-time offer would also fall within the scope of the provision.

The "services" to be offered in the sense of the provision are to be understood to mean any self-employed economic activity which is normally provided for remuneration.[49] Under the GDPR it does not matter whether or not a payment by the data subject is required for the service, i.e. whether the service is rendered for remuneration or free of charge.[50] It is likewise of no relevance where the service is rendered. Accordingly, it makes no difference whether the service offered is provided on the website itself (e.g., download portal, YouTube, Google Street View) or outside of the internet (e.g., in the form of a trip booked via an online travel agency). Services within the meaning of the GDPR are, for example, video streaming services, cloud offerings or social media, online press services or comparison portals. On the other hand, the website of a U.S. company which exists purely for presentational purposes is generally not a service within the meaning of the provision. As the European Data Protection Board made it clear, if a U.S. company delegates employees to the territory of the European Union, the data of these employees will not be processed within the scope of an offer of services within the meaning of Article 3(2) GDPR, but rather for the execution of the employment relationship.[51]

48. Dissenting, presumably, Philip Uecker, *Extraterritorialer Anwendungsbereich der DS-GVO*, 9 Zeitschrift für Datenschutz 67, 70 (2019).

49. *See* Article 4 No 1 of Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market, O.J. L 376/36 (2006).

50. This provision was included in the Regulation at the initiative of the European Parliament, c.f. Legislative Procedure 2012/0011/COD, EP opinion on 1st reading, Am. 20, P7_TA(2014)0212; Article 29 Data Protection Working Party had likewise argued for a similar formulation, *see* Article 29 Data Protection Working Party, *Opinion 01/2012 on the data protection reform proposals*, WP 191, 9 (2012). *See also* European Data Protection Board, *supra* note 19, at 16.

51. European Data Protection Board, *supra* note 19, at 16.

"Goods" within the meaning of the GDPR are all movable tangible objects that can be valued in money and are capable, as such, for forming the subject of commercial transactions.[52] The nature of the transaction involved[53], or the question of whether the objects are of any non-economic value, in particular artistic, historical or ethical-moral, is irrelevant in this regard.[54] Energy sources such as oil, gas or electricity are covered by the term "goods", as are animals, waste, sound recording media and videocassettes. With regard to software, a good is presumed to exist if the associated performance is embodied in an object (e.g., DVDs, hard disks or USB stick). Intangible assets such as computer programs which are detached from material carriers do not comprise goods. Thus, even software which is available on the internet does not meet the definition of a good. However, it may fall under the category of a service.

Additionally, it needs to be "apparent" that the U.S. company envisages offering goods or services.[55] The importance of this prerequisite is not to be underestimated, since it provides an essential corrective against an excessive applicability of the GDPR. Whether or not something is apparently

52. *See* for example ECJ Case 7/68, *Commission v. Italian Republic*, 1968 E.C.R. 423, 428, (*available at* http://curia.europa.eu/juris/showPdf.jsf?text=&docid=87685&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=989038); ECJ Case 1/77, *Robert Bosch GmbH v. Hauptzollamt Hildesheim*, 1977 E.C.R. 1473 (1482).

53. ECJ Case C-2/90, *Commission v. Belgium*, 1992 E.C.R. I-4431, at para. 26, (*available at* http://curia.europa.eu/juris/showPdf.jsf?text=&docid=97067&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=991625); ECJ Case C-324/93, *Queen v. Secretary of State for Home Department*, 1995 E.C.R. I-563, at para. 20, (*available at* http://curia.europa.eu/juris/showPdf.jsf?text=&docid=99176&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=992637).

54. ECJ Case 7/68, *supra* note 52, at 428 et seq.; ECJ Case C-2/90, *supra* note 53, at para. 26; ECJ Case C-324/93, *supra* note 53, at para. 20.

55. *See* recital 23 of the GDPR: "In order to ensure that natural persons are not deprived of the protection to which they are entitled under this Regulation, the processing of personal data of data subjects who are in the Union by a controller or a processor not established in the Union should be subject to this Regulation where the processing activities are related to offering goods or services to such data subjects irrespective of whether connected to a payment. In order to determine whether such a controller or processor is offering goods or services to data subjects who are in the Union, it should be ascertained whether it is apparent that the controller or processor envisages offering services to data subjects in one or more Member States in the Union. Whereas the mere accessibility of the controller's, processor's or an intermediary's website in the Union, of an email address or of other contact details, or the use of a language generally used in the third country where the controller is established, is insufficient to ascertain such intention, factors such as the use of a language or a currency generally used in one or more Member States with the possibility of ordering goods and services in that other language, or the mentioning of customers or users who are in the Union, may make it apparent that the controller envisages offering goods or services to data subjects in the Union."

envisaged must always be examined on a specific case-by-case basis.[56] Only the intention of entering into such commercial relationships with persons in the European Union has to be apparently envisioned, but not the lack of an intention to do so. Therefore, it is generally not necessary to make a "disclaimer" to the effect that an offer is not directed at data subjects who are in the Union. However, it might be advisable to do so.[57] If a disclaimer does in fact exist, for example through a statement by a U.S. company that goods will not be shipped to the EU (e.g., "no overseas shipping"), then the GDPR will clearly not be applicable, unless other circumstances indicate anything to the contrary. The mere accessibility of an English-language website of a U.S. company in the European Union or an e-mail address or other contact details is likewise insufficient to ascertain whether it is "apparent" that the offering of goods or services is "envisaged".[58] The restriction of the provision to an "apparent" intention is not to be ignored by any means, since otherwise a threat of excessive applicability of the GDPR to English-language websites would indeed exist. Nonetheless, this restriction is sometimes not sufficiently appreciated.[59] On the other hand, a use of the English language or of a language or a currency generally used in one or more Member States with the possibility of ordering goods and services in that language, and/or mentioning customers or users who are in the Union, may make it apparent that the controller envisages offering goods or services to data subjects in the Union.[60] An apparent intention exists in particular if services or goods are explicitly offered in one or more Member States which are designated by name or, for example, expenses are incurred for an internet referencing service to the operator of a search engine in order to facilitate access to the provider's website for consumers domiciled in various Member States.[61] Moreover, stating an international area code, using

56. European Data Protection Board, *supra* note 19, at 18.

57. Accordingly, American publishers are already being advised to remove themselves from the scope of the GDPR in particular through disclaimers, but also through other measures; *see* Wimmer, *supra* note 8, at 575 et seq.

58. *See* European Data Protection Board, *supra* note 19, at 18; Wimmer, *supra* note 8, at 552; ambiguous: de Hert & Czerniawski, *supra* note 2, at 239.

59. *See* de Hert & Czerniawski, *supra* note 2, at 241, who do not sufficiently appreciate the restriction to an "apparent" intention and therefore criticize the provision in Article 3(2)(a) GDPR for its perceived broadness.

60. Azzi, *supra* note 2, at 129; Joseph J. Lazzarotti & Mary T. Costigan, *Does the GDPR Apply to Your US-based Company*, NAT'L L. REV. (Jan. 8, 2018), (*available at* https://www.natlawreview.com/article/does-gdpr-apply-to-your-us-based-company); Wimmer, *supra* note 8, at 552 et seq.

61. ECJ Joined Cases C-585/08 and C-144/09, *Peter Pammer v. Reederei Karl Schlüter GmbH & Co. KG* and *Hotel Alpenhof GesmbH v. Oliver Heller*, 2010 E.C.R. I-12527, at para.

a top-level domain specific to a Member State (e.g., ".uk", ".fr", or ".es"),[62] giving directions for travelling from one or more other Member States to the location of the establishment or reproducing customer ratings from the EU can all serve as criteria for the existence of an apparent intention.[63] Another indication that the European Union is being targeted can be that a provider offers a special cost regulation for shipments to Member States of the EU.[64]

3. Case 3: Monitoring the Behavior of Data Subjects in the European Union

Finally, the GDPR also covers data processing by U.S. companies established outside the EU which is related to the monitoring of the behavior of data subjects within the European Union as far as their behavior takes place within the European Union (see Article 3(2)(b) GDPR).

Pursuant to recital 24 of the GDPR, these requirements are met where "natural persons are tracked on the internet including potential subsequent use of personal data processing techniques which consist of profiling a natural person, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes."[65] Consequently, both profiling and tracking in advance of a profiling fall under the GDPR.[66] In the view of the European Data Protection Board, the controller must pursue precisely this specific purpose (i.e.,

81, (*available at* http://curia.europa.eu/juris/document/document.jsf?text=&docid=83437&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=993409); European Data Protection Board, *supra* note 19, at 17. *See* Wimmer, *supra* note 8, at 553 et seq.

62. European Data Protection Board, *supra* note 19, at 18. *See also* the previous version of recital 23 of the GDPR in the 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), Version 56 (29 November 2011), 20; additionally, Paul M. Schwartz, *Information Privacy in the Cloud*, 161 U. PA. L. REV. 1623, 1651 (2013).

63. *See* ECJ Joined Cases C-585/08 and C-144/09, *supra* note 61, at para. 83.

64. *See* Klar, *supra* note 15, at para. 84.

65. *See* recital 24 of the GDPR: "The processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union should also be subject to this Regulation when it is related to the monitoring of the behavior of such data subjects in so far as their behavior takes place within the Union. In order to determine whether a processing activity can be considered to monitor the behavior of data subjects, it should be ascertained whether natural persons are tracked on the internet including potential subsequent use of personal data processing techniques which consist of profiling a natural person, particularly in order to take decisions concerning her or him or for analyzing or predicting her or his personal preferences, behaviors and attitudes."

66. McAllister, *supra* note 3, at 194.

tracking, profiling) with the collection and use of behavior-related data which is defined in recital 24.[67] Accordingly, not every collection or analysis of personal data of persons in the Union which occurs online automatically represents a "monitoring". Thus, for example, the mere setting of cookies by websites for purposes other than those defined in recital 24 does not fall under Article 3(2)(b) GDPR. According to the European Data Protection Board, Article 3(2)(b) GDPR covers in particular monitoring activities such as behavioral advertisement, geo-localization activities (in particular for marketing purposes), online-tracking through the use of cookies or other tracking techniques such as fingerprinting, personalized diet and health analytics online, CCTV, market surveys and other behavioral studies based on individual profiles and monitoring or regular reporting on an individual's health status.[68]

With recital 24 of the GDPR, the regulators make it clear that in contrast to what is being demanded by the European Parliament,[69] the GDPR is explicitly aimed at internet content. Thus, events outside of the internet can in fact not be the subject of a monitoring within the meaning of Article 3(2)(b) GDPR. This means that, for example, monitoring the behavior of data subjects by means of satellite photography, such as Google Earth, would most likely not fall under European data protection law.[70] However, the European Data Protection Board obviously sees this differently and seeks to apply the GDPR to situations which take place outside of the internet as well.[71]

The GDPR does not explain what specific cases are covered by Article 3(2)(b) GDPR.[72] However, it can in any case be derived from that provision that the monitoring must be set up for a specific period of time. One indication of this is the meaning of the word "monitoring", which is characterized by a time component. For another thing, this follows from recital 24 of the GDPR, which explicitly mentions tracking and profiling measures, which can succeed only on the basis of continuous measures.

67. European Data Protection Board, *supra* note 19, at 20; *see also* Wimmer, *supra* note 8, at 557.

68. European Data Protection Board, *supra* note 19, at 20.

69, *See* Legislative Procedure 2012/0011/COD, EP opinion on 1st reading, Am. 7, P7_TA(2014)0212.

70. However, if such photographs are subsequently made accessible on the internet, this form of data processing may well fall under the provision in Article 3(2)(a) GDPR.

71. European Data Protection Board, *supra* note 19, at 19.

72. In view of the insufficient clarity as to which cases were to be covered by this rule, the Article 29 Data Protection Working Party demanded a specification of the provision, *see* Article 29 Data Protection Working Party, *supra* note 50, at 9.

Additionally, the monitoring must have a certain intensity. Measures which are evidently designed from the outset to be one-time and specific actions may not comprise monitoring.[73] On the other hand, the monitoring need not be tantamount to a comprehensive or systematic surveillance, or already make direct decisions which are detrimental to the privacy rights of the data subjects.[74] In fact, the regulators consciously decided against the term "surveillance".[75] The same applies with regard to the French version of the GDPR, which uses the term "observation", but not the word "surveillance". Article 3(2)(b) GDPR also covers data processing activities that occur before specific decisions are made to the detriment of the privacy rights of the data subjects. This follows, from a systemic standpoint, from Article 27(2)(a) GDPR, which stipulates that for cases falling under Article 3(2) GDPR, no representative is to be appointed in the European Union if the data processing will not result in a risk to the rights and freedoms of the data subjects.

It is sufficient if the data processing is objectively suitable for the purpose of the tracking or profiling. Accordingly, even a tracking measure which is carried out against the data subject for the first time and does not recur can lead to an application of Article 3(2)(b) GDPR. On the other hand, the provision does not apply if, for example, the data processing merely serves to deny insecure browsers access to a website.[76]

Since suitability is the decisive factor, the motivation of the controller or processor is of no relevance. Therefore, monitoring is being carried out even if the controller or processor's primary intention is to track the technical processes on its website, but in doing so it processes personal data in a way which would make it possible to track a data subject's internet activities. Consequently, the GDPR covers in particular all forms of tracking and profiling on the internet with the use of analysis tools, such as cookies for example, which enable the tracking of individual users and pursue individualized advertising purposes.[77] Likewise, the application of the

73. As already argued by Manuel Klar, *Räumliche Anwendbarkeit des (Europäischen) Datenschutzrechts – Ein Vergleich am Beispiel von Satelliten-, Luft- und Panoramastraßenaufnahmen*, 3 Zeitschrift für Datenschutz 109, 113 (2013).

74. Critical in this regard: Paul M. Schwartz, *EU Privacy and the Cloud: Consent and Jurisdiction under the Proposed Regulation*, BLOOMBERG BNA PRIVACY & SEC. L. REP. 1, 3 (2013).

75. The draft of the European Commission and that of the Council likewise only mention "monitoring."

76. *See* Schwartz, *supra* note 62*,* at 1652.

77. Doubtful: Wimmer, *supra* note 8, at 555 et seq.

GDPR is triggered by other "value-added services"[78] with which, for example, a cloud provider records the data volume used by its cloud user in order to offer it a larger storage quota if a certain capacity is exceeded.[79] But in each case this requires that the data that are processed in the course of the monitoring have a reference to specific persons.

Article 3(2)(b) GDPR stipulates that the monitored behavior must take place "within the Union". The purpose of this provision is evidently to limit the application of the GDPR to the processing of personal data of those data subjects who are physically within the European Union during the monitoring. As a rule, it can be determined whether or not this is the case by the IP address of the data subject's terminal equipment. Thus, data processing in connection with the use of the internet by a data subject who is in an internet cafe in the U.S. would not fall within the scope of the GDPR. Ultimately, this provision is merely of an informative nature, since the lack of applicability of the GDPR in this exemplary case is already secured by the fact that pursuant to Article 3(2) GDPR, the data subject must be "in the Union".

Since Article 3(2)(b) GDPR does not draw any distinction in this respect, any monitoring of behavior would falls under the scope of the GDPR, regardless of whether or not it is directed at data subjects in the Union.[80] The criterion of apparent envisaging pursuant to recital 23 of the GDPR does not apply in the context of Article 3(2)(b) GDPR – as opposed to Article 3(2)(a) GDPR.[81] It therefore seems to be the case that any website operator using tracking or profiling measures anywhere in the world is obligated to comply with the stipulations of the GDPR. It may be able to evade this obligation by using geo-localization tools in the sense of a "dis-targeting".[82] Thus, no marketplace rule in a narrow sense seems to apply in this regard. The European Data Protection Board therefore advocates a restrictive interpretation of the provision. Accordingly, it explicitly clarifies in its *Guidelines 3/2018 on the territorial scope of the GDPR* that the mere processing of personal data of persons in the Union is not sufficient for the GDPR to be applicable. Rather, the element of "targeting" must also be

78. *See* Schwartz, *supra* note 74*,* at 2.

79. *See* Schwartz, *supra* note 62, at 1644.

80. As is presumably also argued by Peter Schantz & Heinrich A. Wolff, *Das neue Datenschutzrecht*, para. 338 (2017).

81. Svantesson, *supra* note 4, at 71.

82. *See* Svantesson, *supra* note 4, at 99; with regard to "false positives" which would lead to an application of the European legal framework, Svantesson, *A "layered approach" to the extraterritoriality of data privacy laws*, 3 IDPL 278, 284 (2013).

present within the scope of Article 3(2)(b) GDPR.[83] Elsewhere in its Guidelines, it considers it necessary, with reference to recital 24, for the monitoring of the behavior to relate to persons in the Union.[84] This can only be understood to mean that processing within the scope of Article 3(2)(b) GDPR – as already in the case of Article 3(2)(a) GDPR – must be targeted at persons in the Union. However, in that case it is not clear how the further statements of the European Data Protection Board are to be understood, according to which neither Article 3(2)(b) GDPR nor recital 24 introduce a "necessary degree of ‚intention to target'" to determine whether the monitoring activity would trigger the application of the GDPR to the processing activities.[85] Consequently, the statements of the European Data Protection Board are not completely unequivocal. In particular, it remains unclear whether any, and if so what, targeting criteria are supposed to apply, or whether in fact the merely factual use of the tracking and profiling techniques is supposed to represent a "targeting" (also) of persons in the Union. Since the justification for a too broad interpretation would be questionable, the restrictive approach of the European Data Protection Board should definitely be encouraged (even if it would most likely be difficult to support this with the wording of the statute). Without such a restriction, the GDPR would de facto result in a global application. This is why the territorial scope of the GDPR has occasionally been criticized in the legal commentaries on data protection law as "data imperialism" in the past.[86] However, it must also be mentioned in this regard that, even under the former European Directive 95/46/EC, the use of cookies by controllers in third countries had led to the applicability of European data protection law according to the assessment of the Data Protection Working Party.[87] In any

83. European Data Protection Board, *supra* note 19, at 15: "The EDPB also wishes to underline that the fact of processing personal data of an individual in the Union alone is not sufficient to trigger the application of the GDPR to processing activities of a controller or processor not established in the Union. The element of "targeting" individuals in the EU, either by offering goods or services to them or by monitoring their behaviour (as further clarified below), must always be present in addition."

84. European Data Protection Board, *supra* note 19, at 19; and presumably also Wimmer, *supra* note 8, at 557.

85. European Data Protection Board, *supra* note 19, at 20.

86. Critical on this Svantesson, *supra* note 82, 279; Omer Tene & Christopher Wolf, *The Definition of Personal Data: Seeing the Complete Spectrum*, White Paper of the Future of Privacy Forum 3 (2013).

87. Article 29 Data Protection Working Party, *Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based web sites*, WP 56, 10 et seq. (2002). *See* on Article 29 Data Protection Working Party, *supra* note 23.

case, the scope of the provision in practice would most likely be limited by the fact that in many cases there is no obligation to appoint a representative in the Union. Article 27(1) GDPR requires every controller or processor established outside of the European Union to designate a representative in the Union. Under Article 27(2) GDPR, this obligation does not exist if the data processing is occasional, does not include, on a large scale, processing of special categories of data as referred to in Article 9(1) GDPR or processing of personal data relating to criminal convictions and offences and is unlikely to result in a risk to the rights and freedoms of natural persons, taking into account the nature, context, scope and purposes of the processing.[88] These prerequisites are most likely met if a website operator established in the U.S. uses cookies on its English-language website (which is primarily called up in the US, but in a few cases also in the EU) and thereby also covers users in the European Union to a slight extent. Moreover, the possibility cannot be excluded that in such cases, the GDPR would already be inapplicable since the data which are processed do not have a reference to specific persons.[89]

4. Unreasonable Extraterritorial Effects Due to the New Marketplace Rule?

Before the GDPR entered into force, under European Directive 95/46/EC which prevailed at the time, European data protection law applied for controllers established outside of the European Union only if the data processing made use of "equipment, automated or otherwise", which was situated on the territory of the relevant Member State.[90] The only exception to this would be if this equipment was used solely for purposes of transit through the territory of the European Community.[91] Thus, under the previous European Directive 95/46/EC, a territoriality rule applied in this regard

88. The minimum threshold of 250 employees of the controller which was provided for in the European Commission's draft was not included in the final text of the GDPR.

89. With regard to the ECJ's requirement that it be possible to resort to "legal means" in order to connect information to an identifiable natural person, *see* ECJ Case C-582/14, *Patrick Breyer v. Bundesrepublik Deutschland*, 2016 ECLI:EU:C:2016:779, at para. 47 et seq., (*available at* http://curia.europa.eu/juris/document/document.jsf?text=&docid=184668&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=995986). A website operator established in the U.S., for example, could most likely not easily be able to avail itself of such legal means.

90. *See* Article 4(1)(c) Directive 95/46/EC.

91. *See* Article 4(1)(c) Directive 95/46/EC and Moniz, *supra* note 18, at 107.

which proved to be unsatisfactory, particularly with regard to internet matters.[92]

Both criteria were abandoned in the course of the introduction of the GDPR and the establishment of a marketplace rule in Article 3(2) GDPR.[93] The marketplace rule is recognized in the EU in other legal contexts as well, such as European competition and consumer protection law.[94] Beyond that, a recourse to criteria relating to the marketplace is also established in other legal systems and to some extent in the U.S. as well, where a marketplace rule can also be decisive in determining the applicable law. This applies, for example, to domestic matters which only cross state borders.[95] A marketplace rule is also applied in the USA with regard to international matters.[96] For example, the Federal Trade Commission (FTC), which is also responsible for compliance with data protection regulations, avails itself of "targeting" criteria to ascertain the relevant law,[97] with the result that European website operators can also be subject to U.S. data protection provisions.[98] Accordingly, the FTC stressed, for example, that the provisions of the "Children's Online Privacy Protection Act" (COPPA) also apply to

92. *See* Azzi, *supra* note 2, at 128; Moniz, *supra* note 18, at 110.

93. *See also* Schwartz, *supra* note 62*,* at 1643.

94. The conflict of laws provision in Article 6(1) Regulation (EC) No 864/2007 of the European Parliament and of the Council of 11 July 2007 on the law applicable to non-contractual obligations (Rome II), 2007 O.J. L 199/40, explicitly provides with regard to non-contractual obligations arising out of an act of unfair competition that the applicable is that of the country where competitive relations or the collective interests of consumers are, or are likely to be, affected; *see also* Azzi, *supra* note 2, at 129.

95. With regard to the so-called minimum contact test, *see International Shoe Co. v. Washington*, 326 U.S. 310, 316 (1945); on the "Zippo test" in relation to internet matters, *see* Western District of Pennsylvania, 952 F. Supp. 1119 (1997); instructive on the development of the law in the U.S.: Eric C. Hawking, *General Jurisdiction and Internet Contacts: What Role, if any, Should the Zippo Sliding Scale Test Play in the Analysis?*, 74 FORDHAM L. REV. 2371 (2006); Kimberly Houser & Gregory Voss, *GDPR: The End of Google and Facebook or a New Paradigm in Data Privacy?*, 25 RICH. J. L. & TECH. 1, 66 (2018); Alan M. Trammell & Derek E. Bambauer, *Personal Jurisdiction and the Interwebs*, 100 CORNELL L. REV. 1129 (2015).

96. *See* the examples given by Azzi, *supra* note 2, at 132; Houser & Voss, *supra* note 87, at 67 et seq.; Richard Abraham & Colin Loveday, *The General Data Protection Regulation – Another Key Compliance Area for Global Business*, DEFENSE COUNSEL JOURNAL 3, 15 (2018).

97. *See* Bennett, *The "Right to Be Forgotten": Reconciling EU and U.S. Perspectives,* 30 BERKELEY J. INT'L LAW 161, 188 (2012) with further references. *See also* Wimmer, *supra* note 8, at 568 et seq.

98. For a more detailed explanation, see Manuel Klar & Jürgen Kühling, *Privatheit und Datenschutz in der EU und den USA – Kollission zweier Welten?*, 141 Archiv des öffentlichen Rechts 165, 220 (2016).

offers by operators of foreign websites insofar as they are directed at children in the U.S.[99] Finally, the most recently reformed California[100] and Japanese[101] data protection laws also contain a provision which is very similar to the marketplace rule in the GDPR.

The distinguishing feature of the marketplace rule is that it stipulates that the applicable law is that of the place of the final intervention in the market and the place at which the other side of the market is impacted in the sense of a "targeting". As shown above,[102] the contours of the marketplace rule are blurry in some respects.[103] For example, the provisions in Article

99. *See* FTC, *Complying with COPPA: Frequently Asked Questions*, March 2015, (*available at* https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions); *see also* the California Business and Professions Code, whose definition of the term "operator" (*see* 22580 (f) and 22584 (a)) would most likely also include European website operators. In the past, the FTC had already informally written to foreign app providers, calling their attention to their violation of COPPA rules, *see* the FTC's letter of December 17, 2014 to a Chinese app provider, (*available at* https://www.ftc.gov/system/files/documents/public_statements/606451/141222babybusletter.pdf). For more on the extraterritorial effect of COPPA, see Wimmer, *supra* note 8, at 568 et seq.

100. *See* California Civil Code section 1798.140(c): "*(c) 'Business' means:*

(1) A sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners, that collects consumers' personal information, or on the behalf of which such information is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information, that does business in the State of California, and that satisfies one or more of the following thresholds:

(A) Has annual gross revenues in excess of twenty-five million dollars ($25,000,000), as adjusted pursuant to paragraph (5) of subdivision (a) of Section 1798.185.

(B) Alone or in combination, annually buys, receives for the business's commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices.

(C) Derives 50 percent or more of its annual revenues from selling consumers' personal information."; *see also* Lothar Determann, *New California Law Against Data Sharing*, 2 COMPUTER LAW REVIEW INTERNATIONAL 117, 118 (2018).

101. *See* Article 75 of the Amended Act on the Protection of Personal Information (APPI): "The provisions of Article 15, Article 16, Article 18 (excluding paragraph (2)), Article 19 through Article 25, Article 27 thorough Article 36, Article 41, Article 42, paragraph (1), Article 43 and the following Article shall also apply in those cases where a personal information handling business operator who in relation to supplying a good or service to a person in Japan has acquired personal information relating to the person being as a principal handles in a foreign country the personal information or anonymously processed information produced by using the said personal information."

102. *See* II. A. 2. above.

103. As also argued by de Hert & Czerniawski, *supra* note 2, at 239; Philip N. Yannella & Kristen Poetzel, *European Data Protection Board Draft Guidelines on Extraterritorial Scope of the GDPR Provide Few Clear Answers for U.S. Companies*, NAT'L L. REV. (Dec. 1,

3(2) GDPR contain a great deal of new terminology which is not explained any further in either the text of the GDPR or its recitals. Although Article 3 GDPR is a key provision of the GDPR, and its precise scope for companies established outside of the European Union is of decisive importance, there are virtually no indications of the genesis of the provision in the legislative materials. In the legislative notes on the European Commission's draft with regard to Article 3 GDPR, under the heading "Detailed explanation of the proposal" there is merely the cursory remark "Article 3 determines the territorial scope of the Regulation".[104] Although the European Data Protection Board has meanwhile published guidelines on the territorial scope of the GDPR,[105] the specifics are nonetheless disputed, so the scope of the marketplace rule in the future will depend decisively on its interpretation by the ECJ. It has in any case indicated in the recent past that it is by no means contemplating construing the EU data protection requirements restrictively.[106] In its widely noted *Google Spain* decision, it had in fact still based itself on marketplace-related criteria under European Directive 95/46/EC with regard to search engine operators, thus essentially anticipating the new Article 3(2) GDPR.[107] This interpretation of the data protection provisions by the ECJ, taking fundamental rights duly into account, can also be expected to apply now that the GDPR is in effect. In this connection it is to be hoped that the discussion on a balance between data protection and the interests of data processers is approached with a sense of proportion and that the ECJ will see the risk that decisions which are all too hostile to data processing could contribute to European technology companies falling further behind their U.S. competitors economically.

2018), (*available at* https://www.natlawreview.com/article/edpb-draft-guidelines-extraterritorial-scope-gdpr-provide-few-clear-answers-us).

104. European Commission, 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) 11 final version, 7.

105. European Data Protection Board, *supra* note 19.

106. ECJ Case C-210/16, *supra* note 6; ECJ Case C-362/14, *Maximillian Schrems v. Data Protection Commissioner*, 2015 ECLI:EU:C:2015:650; ECJ Case C-131/12, *supra* note 35; ECJ Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*, 2014 ECLI:EU:C:2014:238, (*available at* http://curia.europa.eu/juris/document/document.jsf?text=&docid=150642&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=997468).

107. ECJ Case C-131/12, *supra* note 35, at para. 55. Critical of the decision: Lee A. Bygrave, *A Right to Be Forgotten?*, 58 COMMUNICATIONS OF THE ACM 35, 36 (2015).

Outside of Europe, the marketplace rule of the GDPR largely met with a critical reception[108] and in particular reference was made to the risk that e-commerce would be weakened, since especially small or medium-sized companies which cannot afford the requisite legal expertise would be disadvantaged.[109] In Europe, the aspect of the new approach that received the most praise was the equality of competition between companies in and outside of the European Union.[110] In point of fact, despite some of its technical weaknesses, the marketplace rule in Article 3(2) GDPR represents a middle course. It finds itself between an approach which is linked to the applicability of European data protection law where the controller has its registered office on the one hand (origin approach)[111] and is based on the nationality of the data subject on the other. Inherent to the first alternative is obviously the risk of forum shopping, since a controller could all too easily evade compliance with data protection requirements by choosing a registered office outside of the European Union.[112] In the second case, due to the ubiquity of the internet, every website operator would have to comply with a large number of legal systems simultaneously, since it has no control over who calls up its website. By creating a mediating balance between the two positions, the marketplace rule is theoretically able to resolve the contending interests of the players involved in the data processing in an appropriate manner. Against this background, the regulators correctly refrained from following the approach of taking only the data subject's residence in the European Union as a basis with regard to any and all data processing. In fact, there is no good reason why an EU citizen who, for example, buys a prepaid

108. *See* for example Schwartz, *supra* note 62*,* at 1643; Tene & Wolf, *supra* note 86, at 4; additionally Svantesson, *supra* note 9, at para. 28 and *supra* note 4, at 68 et seq.; Dan Jerker B. Svantesson, *Extraterritoriality and targeting in EU data privacy law: the weak spot undermining the regulation*, 6 IDPL 226, 230 (2015); critical in some respects: de Hert & Czerniawski, *supra* note 2, at 239; Gömann, *supra* note 9, at 588.

109. Cindy Chen, *United States and European Union Approaches to Internet Jurisdiction and their Impact on E-Commerce*, 25 U. PA. J. INT'L ECON. L. 423, 443 (2004).

110. *See* the Study of the Directorate-General for internal Policies, (Direction A), *Reforming the Data Protection Package*, 48 (2012): "This core innovation of the proposal will not only improve the data protection standard within the EU, but also ensure the better functioning of the internal market. By making EU data protection legislation applicable to all providers active within the EU, potential disadvantages which are faced by service providers based within the EU due to its stricter data protection legislation will be ironed out. This would create an EU-wide level playing field and could therefore improve the competitiveness of service providers based within the EU."

111. *See* de Hert & Czerniawski, *supra* note 2, at 235.

112. de Hert & Czerniawski, *supra* note 2, at 235.

card as a tourist in the US, should reap the benefits of European data protection law.[113]

With regard to fundamental rights as well, the marketplace rule would appear to be logical in light of European legal traditions. After all, the state has a protective function both with regard to fundamental rights and under international law.[114] This function is also activated with respect to data processing abroad and requires that state bodies must adequately ensure that the (fundamental) data processing rights are generally safeguarded even when data is processed by foreign entities.[115] This involves the privacy rights of data subjects which are increasingly stressed by the ECJ[116] to the same extent as the creation of competitive equality between European companies and companies in third countries which are active on the European market.[117] Against this background and in particular in light of the provision's clear reference to the EU, expanding the scope of the European data protection requirements would not appear to be inequitable per se.[118] Accordingly, the scope of Article 3(2) GDPR extends to the processing of personal data of data subjects who are "in the Union" and to offers of goods or services "in the Union", as well as to monitored behavior that takes place "within the Union". At least with this approach, it can be ensured that only those matters which actually have a sufficient relationship to the European Union fall under European data protection law.[119] Any ambiguities can be handled with a correspondingly restrictive interpretation of the provision. The applicability of the GDPR should therefore not come as that much of a surprise for U.S. companies, since they are only targeted by it if they target the EU with their activities.[120]

The expansion of the European data protection requirements led many to call attention to the problem of the enforceability of the legal standards.[121]

113. Likewise Moniz, *supra* note 18, at 113.

114. On the existence of state protective duties, also with regard to interventions by foreign countries, see Klar & Kühling, *supra* note 98, at 219.

115. Klar & Kühling, *supra* note 98, at 221.

116. *See supra* note 20.

117. *See* Study of the Directorate-General for internal Policies, (Direction A), *Reforming the Data Protection Package* 48 (2012).

118. Ultimately also de Hert & Czerniawski, *supra* note 2, at 238.

119. Critical of this: de Hert & Czerniawski, *supra* note 2, at 239; Svantesson, *supra* note 9, at para. 28 and *supra* note 108, at 230.

120. de Hert & Czerniawski, *supra* note 2, at 231: "You might be targeted by EU law only if you target."

121. *See* Svantesson, *supra* note 108, at 232, arguing that the GDPR "bites off more than it can chew"; de Hert & Czerniawski, *supra* note 2, at 242; generally critical: Jeffrey Rosen,

They stressed the fact that the data protection authorities would naturally only be able to exert influence within the borders of the European Union and that they could only have the authority to investigate and enforce outside of the EU in accordance with interstate treaties which as yet do not exist, thus limiting their options for action outside of the European Union per se.[122] However, law which cannot be enforced would serve no purpose.[123] Along these lines, the Data Protection Working Party also stated already with regard to former European Directive 95/46/EC that the data protection laws should (only) be applicable "where it is necessary, where it makes sense and where there is a reasonable degree of enforceability having regard to the cross-frontier situation involved."[124] The enforcement of the GDPR's rules should in any case be facilitated by the fact that pursuant to Article 27(1) GDPR, every controller or processor established outside of the European Union has to designate a representative in the Union.[125] Under Article 27(2) GDPR, this obligation ceases to apply only if the data processing is carried out on an occasional basis, does not cover any special categories of personal data within the meaning of Article 9(1) GDPR or data relating to criminal convictions and offences pursuant to Article 10 GDPR and it is unlikely to result in a risk to the rights and freedoms of natural persons, taking into account the nature, context, scope and purposes of the processing. Moreover, a violation of the duty to appoint a representative pursuant to Article 83(4)(a) GDPR is now subject to a fine, which was not the case previously.[126]

B. Material Scope

In order for the GDPR to apply for U.S. companies, they must fall not only within the territorial scope described above, but within its material scope as well, which is defined in Article 2 GDPR. In addition to the stipulations on the territorial applicability of the GDPR, this provision represents a further key standard for its applicability, as it applies only for the processing of personal data wholly or partly by automated means (Article 2(1) GDPR). On the other hand, it does not apply if personal data are merely

The Right to Be Forgotten, 64 STAN. L. REV. ONLINE 88, 92 (2012): "Europeans have a long tradition of declaring abstract privacy rights in theory that they fail to enforce in practice."

122. de Hert & Czerniawski, *supra* note 2, at 242.

123. Tene & Wolf, *supra* note 86, at 4; *see also* Bygrave, *supra* note 107, at 252.

124. Article 29 Data Protection Working Party, *supra* note 87, at 9.

125. *See also* Azzi, *supra* note 2, at 133.

126. For more information on the representative, see under V. A.

processed by natural persons in the course of a purely personal or household activity (so-called "household exemption").[127]

The questions of what prerequisites are to be placed on the criterion of "automated and non-automated processing" and how the term "personal data" and the criteria for "household exemptions" are to be interpreted will be taken up in the following section.

1. Automated and Non-Automated Processing

The GDPR only applies in a material sense where personal data are processed wholly or partly by automated means (Article 2(1) GDPR). For non-automated processing, the GDPR applies only if the personal data are contained or are intended to be contained in a filing system.[128]

Thus, it must first of all be ascertained how the GDPR's use of the term "processing" is to be understood. In its definition of "processing" in Article 4 no. 2, the GDPR summarizes a great many forms of processing. The term "processing" means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means. The first step in an ideally typical processing procedure would be the collection or recording of personal data. This can be followed by the organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination or restriction of the data. Finally, there is the erasure or destruction of the personal data.

If (as in most situations), a processing is taking place, it must be ascertained whether it is being carried out wholly or partly by automated means. Here, it must be taken into account that even for a non-automated processing of personal data, Article 2(1) GDPR stipulates that the GDPR is applicable insofar as the information is contained, or is intended to be contained in a filing system. A processing wholly or partly by automated means is always present if data processing equipment is used. The GDPR does not provide a specific definition of an automated processing with the use of data processing equipment, let alone any examples. This is to be understood as a deliberate decision, since the GDPR is also supposed to cover future technological developments.[129] It is of no relevance in connection with automated processing whether the files are stored in any

127. *See* Article 2(2)(c) GDPR.

128. *See* JÜRGEN KÜHLING & MANUEL KLAR & FLORIAN SACKMANN, DATENSCHUTZRECHT 99 (4th ed. 2018).

129. *See* recital 15 of the GDPR.

structured manner. The distinction between a wholly or partly automated processing is to be drawn on the basis of possible manual interim steps.[130] For example, a partly automated processing is present if the data are collected by a person, and not directly by a data processing system.

Along with data processing that is carried out wholly or partly by automated means, the scope of the GDPR additionally also covers the non-automated processing of personal data subject to certain prerequisites. According to recital 15, the term non-automated processing in the GDPR is understood to mean purely manual processing. Since it is already sufficient for an assumption of partly automated processing if an individual partial step is carried out automatically, this would mean conversely that in manual processing, no processing steps may be automated at all. The main case in which non-automated processing would apply would most likely be when information is recorded, for example with a pen on a sheet of paper. The GDPR restricts its scope with regard to manual processing such that it is applicable only if the information is contained or is intended to be contained in a filing system. Pursuant to Article 4 no. 6 GDPR, this would mean any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis. Accordingly, pursuant to recital 15 of the GDPR, files or sets of files, as well as their cover pages, which are not structured according to specific criteria should not fall within the scope of the GDPR. Such criteria could perhaps be a classification by year, file number or name, for example in alphabetical order. As a rule, a collection could be referred to as a structure if it can be sorted according to more than two criteria. According to the ECJ, a "filing system" covers a set of personal data, if those data are structured according to specific criteria which, in practice, enable them to be easily retrieved for subsequent use.[131]

2. Personal Data

What is also of key importance for the applicability of the GDPR is whether the U.S. company processes "personal data".[132] Since the term "personal data" is very broadly construed in European law, in some cases this results in very clear differences from the semantic definitions under U.S.

130. *Kühling & Klar & Sackmann, supra* note 128, at 101.

131. ECJ Case C-25/17, Jehovah's Witnesses, 2018 ECLI:EU:C:2018:551, (*available at* http://curia.europa.eu/juris/document/document.jsf?text=&docid=203822&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=2129026).

132. On the term "personal data," *see* Manuel Klar & Jürgen Kühling, in DS-GVO/BDSG, Art. 4 Nr. 1 DS-GVO (Jürgen Kühling & Benedikt Buchner, 2nd ed. 2018).

law which, for example, unlike the GDPR, does not classify publicly accessible data as personal.[133]

According to the GDPR, personal data comprise any information relating to an identified or identifiable natural person (Article 4 no. 1 GDPR). A identifiable person should already be considered to be one who can be identified, directly or indirectly, in particular by reference to an identifier, such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Personal data are only information which relates to a natural person. The GDPR defines these persons as "data subjects". Legal entities, as well as groups of persons, are excluded from the scope of protection. However, where information on a group of persons "spills over" to an identified or identifiable member, this information comprises personal data.[134] That can be the case, for example, if a statement is made on the financial situation of a partnership or a "one-person company."

Article 4 no. 1 GDPR comprehends without restriction "any information" relating to a person and is therefore to be understood broadly. This provision covers both personal information used in context such as identifiers (e.g., name, address and date of birth), external factors (such as gender, eye color, height and weight) or internal conditions (e.g., opinions, motives, desires, convictions and value judgments), as well as objective information such as financial and ownership situation, communication and contractual relationships and all other relationships of the data subjects to third parties and their environment. The significance or privacy law implication of the information is of no relevance. Even the information that person X has two arms comprises personal data within the meaning of Article 4 no. 1 GDPR.

Pursuant to Article 4 no. 1 GDPR, the information must "relate" to a natural person. So-called "data related to things" do not pertain to a person, but merely to a thing. This is the case, for example, with the statement

133. *See, e.g.*, California Civil Code section 1798.140(o)(2): "'Personal information' does not include publicly available information. For these purposes, 'publicly available' means information that is lawfully made available from federal, state, or local government records, if any conditions associated with such information. 'Publicly available' does not mean biometric information collected by a business about a consumer without the consumer's knowledge. Information is not 'publicly available' if that data is used for a purpose that is not compatible with the purpose for which the data is maintained and made available in the government records or for which it is publicly maintained. 'Publicly available' does not include consumer information that is deidentified or aggregate consumer information."

134. *See* Article 29 Data Protection Working Party, *Opinion 4/2007 on the concept of personal data*, WP 136, 23 (2007) with regard to the earlier European Directive 95/46/EC.

"Mount Everest is the highest mountain on Earth" or "House X costs 400,000 dollars". This applies even if a U.S. company or a third party is aware that Person A has climbed Mount Everest or is the owner of house X. However, a great number of contentious cases would be conceivable under European law which would require a nuanced solution in each individual case. Demarcation issues arise above all in connection with machine-to-machine communication by everyday objects which are connected to the internet, such as vehicles, kitchen appliances or wearables ("Internet of Things"). As a rule, these are not to be considered to be data related to things. Data related to things can be differentiated from personal data by taking the context-related approach, which the Data Protection Working Party had developed to the term "personal data" under the preceding European Directive 95/46/EC. It stated that information relates to a natural person (and not to a thing), if a content element, a purpose element or a result element is present.[135] A content element exists where information is given about a person which is to be assessed in light of all circumstances surrounding the case and regardless of any purpose on the part of the data controller or a third party or the impact of that information on the data subject. A purpose element exist if the information can be used for the purpose of evaluating a person, treating them in a certain way or influencing them. Finally, even if no content or purpose element exists, a result element will always exist if there is a risk that the information, in light of all circumstances surrounding the case, can have an impact on a certain person's rights and interests. This can be the case, for example, with information on the economic utilization and exploitation of real estate.

Pursuant to Article 4 no. 1 GDPR, the information must relate to an "identified or identifiable" person. An identified person is one who can be identified directly from the information itself.[136] This is the case, for example, if the information contains an identifier (e.g., name, address and date of birth) of the person or the content of the information or the context allow for the unique identification of that person without the need to make use of additional information. On the other hand, a person is identifiable if the information in and of itself is not sufficient to attribute it to a person, but this is possible once the information is linked to additional information.[137] Pursuant to recital 26 of the GDPR, in order to determine whether a person is identifiable, account should be taken of all the means reasonably likely to

135. *See* already on European Directive 95/46/EC Article 29 Data Protection Working Party, *supra* note 134, at 9.

136. ECJ Case C-582/14, *supra* note 89, at para. 38.

137. *Klar & Kühling*, *supra* note 132, at para. 19.

be used either by the controller or by another person to identify the natural person directly or indirectly. Identifying these means requires, according to recital 26 of the GDPR, that all of the information that is known or available about the data subject, as well as all objective factors, such as the cost of and amount of time required for identification, be taken into account. The extent to which the knowledge and means of third parties which can be used to identify a person are also to be taken into account is disputed. The ECJ has found that a reference to specific persons exists in connection with IP addresses if and insofar as the website operator has the legal means to access the data of the third parties, i. e. the internet service provider.[138] However, possibilities for doing so which are prohibited by law should not come into question.[139]

A subcategory of personal data is pseudonymous data. This includes data which are processed in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information (cf. Article 4 no. 5 GDPR). This definition is similar to that in the California Consumer Privacy Act of 2018, which contains a similar definition of the term.[140] With regard to the additional information, it must be ensured that it is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person. Characteristic for pseudonymous data is thus – in contrast to anonymous data (see below) – the existence of an attribution rule which provides the data collected under a pseudonym with an identifier of a person. As Article 32(1)(a) GDPR clarifies, pseudonymization is merely a security measure.[141]

Anonymous data do not fall under the category of personal data. Accordingly, as set out in recital 26 of the GDPR, the principles of data protection law **do not apply for anonymous information**. The question of whether a natural person is no longer identifiable and the data are thus anonymous must be examined in accordance with recital 26 of the GDPR, i.e. account should be taken of all the means reasonably likely to be used

138. *See* ECJ Case C-582/14, *supra* note 89, at para. 47 et seq.

139. ECJ Case C-582/14, *supra* note 89, at para. 46.

140. California Civil Code section 1798.140(r): "'Pseudonymize' or 'Pseudonymization' means the processing of personal information in a manner that renders the personal information no longer attributable to a specific consumer without the use of additional information, provided that the additional information is kept separately and is subject to technical and organizational measures to ensure that the personal information is not attributed to an identified or identifiable consumer."

141. Likewise already Article 29 Data Protection Working Party, *Opinion 05/2014 on Anonymisation Techniques*, WP 216, 3, 10 (2014).

either by the controller or by another person to identify the natural person directly or indirectly, whereby in particular the cost of and amount of time required for identification are to be taken into account. The GDPR does not stipulate what technical requirements have to be met by an anonymization. However, recital 26 of the GDPR does provide that when ascertaining whether a person is identifiable, the available technology at the time of the processing and technical developments must be taken into account. Consequently, the anonymization procedure used must at least be in accordance with the current state of the art.

3. Household Exemption

Another exceptional case, which is known as the "household exemption", is regulated in Article 2(2)(c) GDPR, under which data processing is not subject to the GDPR if it is carried out by a natural person in the course of a purely personal or household activity. The GDPR does not provide a specific definition or demarcation of the terms "personal" or "household" activity. This exception is an expression of the fact that the private sphere is generally protected in Europe by fundamental rights.[142] One criterion for demarcation formulated by recital 18 of the GDPR is the lack of any connection whatsoever to a professional or commercial activity, and it cites as examples of personal and household activities correspondence and the holding of addresses, or social networking and online activity undertaken within the context of such activities. Whether or not data processing is of a personal or household nature is determined according to generally accepted standards. With regard to the social networking that is cited in recital 18 of the GDPR, a nuanced examination is necessary on the basis of the criterion of accessibility.[143] As long as the use is carried out in such a way that a merely limited group of persons obtains knowledge of information, such as in the course of individual or group messages, however, the exception can be applicable.[144]

However, the exception does not apply for the publication of information for an indeterminate group of people. The ECJ has already taken

142. *See Kühling & Klar & Sackmann, supra* note 128, at 102-103.

143. European Data Protection Supervisor, Executive summary EDPS Opinion of 7 March 2012 on the data protection reform package, 2012/C 192/05, 2012 O.J. C 192/7, 9.

144. Jürgen *Kühling & Johannes Raab*, in DS-GVO/BDSG, Art. 2 DS-GVO para. 25 (Jürgen Kühling & Benedikt Buchner, 2nd ed. 2018).

a position on this point in its *Lindqvist*[145] and *Satamedia*[146] judgments and does not subsume a public disclosure under the corresponding exception set out in Directive 95/46/EC (which was still in force at the time). Despite mentioning social networking in its recitals, the GDPR does not seek to derogate from this case law. However, since this point has not been clarified in the legislative process, it is to be expected that ECJ will take it up further. But even if private or household processing is covered by the exception in a specific case, the providers of such internet platforms cannot likewise invoke the exception for themselves that is applicable to its users. This is made clear by recital 18 of the GDPR at the end where it places the controllers which provide the means for processing the users' data within the scope of the GDPR. Moreover, the wording of the provision is very narrow in that it requires a use "purely" for the purpose of personal or household activities. Thus, the exception does not apply to **mixed data collections**, such as address books, which contain both private and business contacts. A video surveillance of the private sphere can also be covered by the exception since the security and safety of one's own home is to be deemed to be a private purpose. However, according to a more recent decision of the ECJ, this does not apply if at the same time a public area, such as the street in front of the house, is also recorded.[147]

III. Applicability of National Data Protection Law of the EU Member States

Along with the possibility of being directly bound by the stipulations of the GDPR (see II. above), U.S. companies can also be subjected to certain data protection regulations which are enacted not by the European legislature but by the Member States of the European Union whose territorial scope might also extend to U.S. companies.

145. ECJ Case C-101/01, Lindqvist, 2003 ECLI:EU:C:2003:596, (*available at* http://curia.europa.eu/juris/document/document.jsf?text=&docid=48382&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=998664).

146. ECJ Case C-73/07, *Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy and Satamedia Oy*, 2008 ECLI:EU:C:2008:727, at para. 43 et seq., (*available at* http://curia.europa.eu/juris/document/document.jsf?text=&docid=76075&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=999192).

147. ECJ Case C-212/13, *František Ryneš v Úřad pro ochranu osobních údajů*, 2014 ECLI:EU:C:2014:2428, at para. 33, (*available at* http://curia.europa.eu/juris/document/document.jsf?text=&docid=160561&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=999597); cf. Manuel *Klar*, *Private Videoüberwachung unter Miterfassung des öffentlichen Raums*, 68 Neue Juristische Woche 463 (2015).

For example, the GDPR contains a rather large number of opening clauses which make it possible for individual Member States to specify the provisions of the GDPR in national data protection provisions with regard to various matters. Such possibilities to specify exist, for example, in the areas of employee data protection,[148] scientific research,[149] processing for journalistic, scientific, artistic or literary purposes,[150] the processing of sensitive data[151] or within the scope of Article 23 GDPR, which contains a comprehensive and general opening clause allowing the Member States and the European Union to derogate from the GDPR's provisions and further restrict the rights of data subjects.

The harmonizing effect of the GDPR in the Member States of the European Union is called into question to a great extent by these opening clauses. They ultimately resulted from a compromise between the legislative bodies, since in the new era of the GDPR many Member States have sought to "keep alive" to the greatest possible extent their data protection regulations which had existed up to the applicability of the GDPR, and of which they had become very fond. However, extensive national regulations jeopardize the actual harmonization objective of the GDPR, namely the elimination of the "patchwork quilt" of national data protection regimes which had existed up to the applicability of the GDPR on May 25, 2018. Moreover, each time a Member State avails itself of opening clauses, the question of whether its provisions are in conformity with EU law arises, which then gives rise to legal uncertainty in this regard.

Furthermore, if the Member States make use of these opening clauses, it is largely unclear whether, and if so on what basis, these sectoral requirements can lay claim to validity outside of the borders of the respective Member State.[152] The GDPR does not contain any provisions with regard to the territorial scope of national data protection regulations which are enacted on the basis of the GDPR's opening clauses, even though the European Data Protection Supervisor had called attention to this failing at an early stage.[153] Article 3 GDPR does not apply in this regard, even analogously. This leads to a considerable degree of legal uncertainty for U.S. companies, since it will

148. *See* Article 88 GDPR.

149. *See* for example Article 89 GDPR.

150. Article 85(2) GDPR.

151. *See* Article 9(2)(a) GDPR.

152. *See* Klar, *supra* note 15, at para. 107.

153. *See* European Data Protection Supervisor, *supra* note 143, 9. The European Data Protection Supervisor acts as a supervisory authority specifically for the institutions and bodies of the EU (*see* Article 16(2) sentence 2 of the Treaty of the Functioning of the European Union – TFEU).

often not be entirely clear when the national data protection regulations actually have extraterritorial validity. This is the case, for example, with regard to the German provisions in section 1(4) sentence 2 no. 1 of the German Federal Data Protection Act *(Bundesdatenschutzgesetz – BDSG),* the repercussions of which are quite simply absurd as far as extraterritorial matters are concerned.[154] Under this provision, German data protection law applies if, for example, a U.S. company has personal data processed by a computer or even merely a server in Germany. Under certain circumstances this can in fact lead to an unfortunate situation in which even though the U.S. company does not fall under the provisions of the GDPR (see above), it nonetheless has to comply with the requirements of the German Federal Data Protection Act, which actually was only supposed to make the GDPR's requirements more precise. Here too, it can only be hoped that the European and national legislatures will recognize the need for adjustment and fine-tune their respective regulations accordingly in their next "revision round".

IV. Contractual Subjection to the Rules of the GDPR

Along with a direct subjection to the European data protection requirements (see above under III.), situations can arise in which U.S. companies are only indirectly confronted with them. This is the case if European contracting parties urge the conclusion of certain data protection contracts which are mandatory in certain situations due to the GDPR, and the EU undertaking could face a fine if it does not meet this requirement.[155] In such cases, even if they do not have to comply with the GDPR directly, U.S. companies could at least be contractually obligated to meet the data protection level stipulated by the GDPR. Here it should be noted that the contents of these contracts are frequently explicitly stipulated and changes are only possible to a limited extent. This can have a direct impact on the understanding of the respective other contracting party in the course of contractual negotiations. The following contractual scenarios would come into consideration in this regard.

154. Pursuant to section 1(4) sentence 2 no. 1 of the German Federal Data Protection Act, the provisions of the Act apply to all public bodies if the controller or processor processes personal data in Germany. Consequently, this regulation links to the location of the data processing and thus bases itself on a criterion which the European legislators had in any case deliberately avoided with regard to the GDPR. In this regard, the provision is in direct conflict with the approach taken by EU law.

155. *See* Article 83(4)(a) GDPR.

A. Agreement on Commissioned Data Processing

If U.S. companies act as so-called processors for European companies, EU companies are required by mandatory law to conclude a contract on commissioned data processing with the U.S. company (see Article 28(3) GDPR).[156]

Commissioned data processing is present if a natural or legal person processes personal data on behalf of a controller (see Article 4 No. 8 GDPR). Accordingly, the decisive factor is the commissioning of personal data processing where the contractor is not itself a "controller" within the meaning of Article 4 No 7 GDPR. Unlike a controller, a processor does not determine the purposes and means of the data processing, but merely processes the data strictly as instructed for the purposes set by the principal. Typical examples of processors are IT service providers in the areas of hosting, Software as a Service (SaaS), other cloud services or call centers which collect customer data as stipulated by the principal and only for its business purposes (e.g. conclusion of contracts or handling of complaints). German supervisory authorities have found in the past that commissioned data processing is also present with regard to the use of Google Analytics,[157] whereas they have recently taken the view that Google is to be regarded as a controller rather than a processor because it processes personal data for its own purposes.

The content of an agreement on commissioned data processing is described in a fairly detailed manner in Article 28(3) GDPR. For example, the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the respective company have to be set out. Moreover, the contract must in particular stipulate that the personal data of the U.S. company may only be processed at the documented instruction of the EU company, that it is ensured that persons authorized to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality, that all necessary technical and organizational measures are taken and that the particular requirements of the GDPR regarding the engagement of other processors are complied with. Furthermore, it must stipulate that the EU company is to be assisted in ensuring compliance with its obligations under the GDPR and that

156. *See also* Christian M. Auty, *How The GDPR Will Affect U.S. Data "Processors"*, NAT'L L. REV. (Mar. 5 2018), (*available at* https://www.natlawreview.com/article/how-gdpr-will-affect-us-data-processors).

157. *See* Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit, *23rd Tätigkeitsbericht Datenschutz 2010/2011*, 177.

the U.S. company will make available to the EU company all information necessary to demonstrate compliance with the obligations laid down in Article 28 GDPR and allow for audits and inspections. After the end of the provision of the processing services, all of the personal data must be deleted or returned at the choice of the EU company – this too is to be set out in the contract. As the detailed list of minimum requirements shows, when structuring a contract on commissioned data processing, there is not that much leeway for drafting individual provisions.

It is not entirely insignificant that in the view of the European Data Protection Board, a contract must also be concluded if the situation is reversed, i.e., if a EU company acts as a processor for a U.S. company. However, in the assessment of the European Data Protection Board, the obligations set out in Article 28(3) GDPR in this regard would have to be modified to reflect the special situation that the U.S. company is not subject to the GDPR and it would therefore not make any sense for the processor to assist the U.S. company in complying with the requirements under the GDPR.[158]

Finally, it is of significance that a contract on commissioned data processing also needs to be concluded even if the U.S. company is certified under the EU-US Privacy Shield.[159] Nor does the conclusion of standard contractual clauses of the European Commission suspend an agreement on commissioned data processing pursuant to Article 28(3) GDPR – or vice versa.[160] This can be extremely irritating, since the provisions strongly

158. European Data Protection Board, *supra* note 19, at 12: "When it comes to a data processor established in the Union carrying out processing on behalf of a data controller with no establishment in the Union for the purposes of the processing activity and which does not fall under the territorial scope of the GDPR as per Article 3(2), the processor will be subject to the following relevant GDPR provisions directly applicable to data processors: (...) The obligations imposed on processors under Article 28 (2), (3), (4), (5) and (6), on the duty to enter into a data processing agreement, with the exception of those relating to the assistance to the data controller in complying with its (the controller's) own obligations under the GDPR."

159. As is presumably also the opinion of the European Data Protection Board, *supra* note 19, at 11.

160. This is most likely also in line with the assessment of the European Data Protection Board, *supra* note 19, at 13. However, the problem with this scenario in which the EU company acts as a processor for a U.S. company is that no standard clauses exist (yet) for this case. The standard contractual clauses of the European Commission which are available to date apply only to cases in which a EU company as the controller transfers personal data to a processor outside of the EU, *see* European Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council, C(2010) 593, 2010 O.J. L 39/5.

resemble each other in many points. In practice this frequently leads to conflicts in priority between the different regulations. However, these conflicts are ultimately inherent to the GDPR and can therefore scarcely be sensibly resolved – this can be remedied only by the regulators or clarifications by the authorities.

B. Joint Controllership Agreement

If the EU company and the U.S. company are deemed to be "joint controllers" pursuant to Article 26 GDPR, the EU company is in any case required by mandatory law to conclude a joint controllership agreement. Here too, parts of the European data protection law are extended by contract to U.S. companies.

A joint controllership agreement is required if two data processing bodies are to be deemed to be joint controllers for the processing within the meaning of Article 26 GDPR. This is the case if two or more controllers under data protection law jointly determine the purposes and means of the processing of personal data. In the view of the ECJ, a joint controllership is indicated if a natural or legal person exerts influence over the processing of personal data of another for his own purposes, thus participating in the determination of the purposes and means of that processing.[161] At the same time, it believes that a joint controllership does not necessarily imply equal responsibility. Rather, the actors involved can be incorporated into the relevant processing in various phases and to different extents, and thus the degree of the responsibility of each of them is to be evaluated in consideration of all of the decisive circumstances of the individual case.[162] According to the ECJ, it would not be necessary for each of the actors to have equivalent access to the relevant personal data.[163] In the assessment of the ECJ, a joint controllership would in any case come into consideration for such processing steps if the decisions on their purpose and means are actually made jointly.[164] In the past, the ECJ held that a joint controllership exists, for example, between Facebook and the administrator of a Facebook Fanpage.[165] A joint controllership can also be assumed, in the view of the German data

161. ECJ Case C-25/17, Jehovah's Witnesses, *supra* note 6. For more on the criteria, see *also* Article 29 Data Protection Working Party, *Opinion 1/2010 on the concepts of "controller" and "processor"*, WP 169, 17 (2010).

162. ECJ Case C-210/16, Facebook Fanpages, *supra* note 6.

163. ECJ Case C-210/16, Facebook Fanpages, *supra* note 6; ECJ Case C-40/17, Fashion ID, *supra* note 6.

164. ECJ Case C-40/17, Fashion ID, *supra* note 6.

165. *See* ECJ Case C-210/16, Facebook Fanpages, *supra* note 6.

protection authorities, in the case of clinical medical trials if multiple participants (e.g., sponsor, study centers/physicians) each make decisions on the processing in their respective areas.

If a joint controllership exists, the arrangement that is then to be concluded must regulate the respective roles and relationships of the joint controllers vis-à-vis the data subjects.[166] Moreover, it must be established which of the joint controllers must fulfill what obligation under the GDPR, in particular with regard to the perception of the rights of the data subjects and who will have to fulfill which duties to provide information under Articles 13 and 14 GDPR.[167] Finally, the essence of the arrangement must be made available to the data subjects.[168] Notwithstanding the allocation of the duties internally between the joint controllers, however, the data subjects can assert their rights against each of the joint controllers individually.[169]

It is of considerable practical relevance that a joint controllership agreement also needs to be concluded even if the U.S. company is certified under the EU-US Privacy Shield.[170] The same applies where standard contractual clauses of the European Commission are to be concluded pursuant to Article 46(2)(c) GDPR (more on this below).[171]

Finally, it is of importance with regard to a joint controllership that in the event of an unlawful processing, each of the joint controllers would be liable for the entire damage unless it can provide proof that it was not at fault.[172] Even without an arrangement on joint controllership, the joint controllers bear jointly and several liability. However, the arrangement can provide for regulations on an equalization of liability in the internal relationship between the parties.[173] It should be noted that joint and several liability is unlikely to apply if the U.S. company does not fall within the scope of the GDPR (see above).

166. *See* Article 26(2) sentence1 GDPR.

167. Article 26(1) sentence 2 GDPR.

168. *See* Article 26(2) sentence 2 GDPR.

169. Article 26(3) GDPR.

170. As is presumably also the opinion of the European Data Protection Board; *supra* note 19, at 11.

171. This would most likely also follow from the opinion of the European Data Protection Board; *see supra* note 19, at 12.

172. *See* Article 82(4) in conjunction with (2) sentence 1 and Article 82(3) GDPR.

173. Article 82(5) GDPR.

C. Standard Contractual Clauses of the European Commission

Additionally, U.S. companies can be contractually subjected to European data protection law if the EU company employs the so-called "standard contractual clauses" of the European Commission to secure the transfer of data to the US. The reasoning behind this is that under Articles 44 et seq. GDPR, European companies have to secure data transfers to recipients outside of the EU by means of special instruments if the European Commission has not determined that the third country offers an adequate level of data protection, as is the case with the US. If the U.S. company receiving the data is not certified under the "EU-U.S. Privacy Shield", agreeing to the standard contractual clauses pursuant to Article 46(2)(c) GDPR often offers a quick and practical means in practice to structure the data transfer in a lawful manner.

The European Commission had already issued corresponding regulations when European Directive 95/46/EC was still in force, namely one version of standard contractual clauses for exchanges between a controller and a processor (controller-processor transfer)[174] and another to be used between controllers (controller-controller transfer).[175] These regulations will continue to apply under the GDPR until they are amended, replaced or repealed.[176]

A particular advantage of standard contractual clauses is the fact that they involve standardized agreements which can, and may, no longer be amended or negotiated. Nor is a separate approval by an authority required. Therefore, in practice standard contractual clauses are both popular and widespread. However, it is not clear how long that will continue to be the case. The judgment of the ECJ in the *Schrems*[177] case, in which it declared the previous safe-harbor decision of the European Commission of 2000 to be invalid, will most likely also have repercussions on the current standard contractual clauses which are presently being examined by the ECJ.[178] The

174. European Commission Decision, *supra* note 160.

175. European Commission Decision of 27 December 2004 amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries, C(2004) 5271, 2004 O.J. L 385/74.

176. *See* Article 46(5) sentence 2 GDPR.

177. ECJ Case C-362/14, *supra* note 106.

178. *See* the Judgment of the Irish High Court of 3 October 2017 to submit standard contractual clauses to the ECJ for its review, Judgment 2016 No. 4809 P. (*available at* http://www.europe-v-facebook.org/sh2/HCJ.pdf).

"half-life" of the standard contractual clauses that are still valid at the moment is therefore likely to be limited.

The standard contractual clauses regulate the rights and duties of the data exporter (i.e., the EU company) and the data importer (i.e., the U.S. company). They also contain provisions regarding the commissioning of additional subcontractors and on liability. The parties must describe the essential content of the transfer in the annexes to the standard contractual clauses (categories of the data transferred, data subjects, purposes of the transfer, processing measures, etc.). These are the very few parts of the standard contractual clauses which can (and must) be adjusted by the contracting parties.

It should be noted that the contracts that must be entered into in the case of a joint controllership within the meaning of Article 26 GDPR or a commissioned data processing pursuant to Article 28 GDPR (which was discussed above) must be concluded in addition to the standard contractual clauses, which can lead to conflicts in priority.[179] Another problem that arises in the case of a commissioned data processing is that an EU processor is obligated under Articles 44 et seq. GDPR to comply with the requirements for the permissible transfer of data to third countries.[180] However, it must be noted in this connection that at present there is no set of standard contractual clauses of the European Commission which could be concluded directly between an EU processor and a U.S. company. The standard contractual clauses of the European Commission which are available to date apply only to cases in which an EU company as the controller transfers personal data to a processor outside of the EU.[181] It is therefore absolutely essential that this legal situation be further developed, either by the ECJ or by clarifying official statements.

V. Consequences for U.S. Companies which are Subject to the GDPR

If a U.S. company falls under the GDPR, it must comply with the provisions therein to the same extent as an EU company which is bound to the stipulations of the GDPR. There is no "layered approach" in this regard.[182] If the company offers goods or services to persons in the European Union or monitors their behavior, it must appoint a representative in the

179. *See* IV. A. and IV. B. above.

180. European Data Protection Board, *supra* note 19, at 13.

181. *See* European Commission Decision, *supra* note 160.

182. Proposing such an approach: Svantesson, *supra* note 9, at para. 33.

European Union (see A.). With regard to the other duties which are to be fulfilled, a distinction must be made as to whether the U.S. company is acting as a controller or as a processor within the meaning of the GDPR. Independent of that, the U.S. company will then have to comply with a great many other duties, breaches of which are subject to fines (see B.). However, it must be pointed out that at present it is still completely unclear whether, and if so how, a breach of these duties by U.S. companies would be prosecuted by European supervisory authorities.

A. Appointment of a Representative in the EU

In the cases set out in Article 3(2) GDPR, i.e., if U.S. companies offer goods or services in the EU or monitor their behavior, the controller or processor must designate a representative in the European Union in writing.[183] However, this does not apply for processing which is occasional, does not include, on a large scale, processing of special categories of data as referred to in Article 9(1) GDPR or processing of personal data relating to criminal convictions and offences referred to in Article 10 GDPR, and is unlikely to result in a risk to the rights and freedoms of natural persons, taking into account the nature, context, scope and purposes of the processing.

The representative must be established in one of the Member States where the data subjects are whose personal data are being processed in relation to the offering of goods or services to them, or whose behavior is being monitored. The representative must be mandated by the U.S. company to be addressed in addition to or instead of the controller or the processor by supervisory authorities and data subjects, on all issues related to processing, for the purposes of ensuring compliance with the GDPR.

According to recital 80 of the GDPR, the conception is to make it possible for the representative to be addressed by any supervisory authority. This is not only meant to facilitate the communication and serving of actions or injunctions against the controller or the processor. Article 58(1)(a) GDPR provides that in cases of violations of data protection law, the controller, the processor "and where applicable", the controller's or the processor's representative must also provide information. This is accompanied by recital 80 of the GDPR, under which the representative can be subject to enforcement proceedings. How specifically the implementation of these provisions against U.S. companies will be structured will depend decisively on the data protection authorities' intention to enforce them and their ability to create a potential to apply pressure, as well as on the willingness of the

183. *See* Article 27 GDPR.

relevant data processing companies to cooperate with them. Ultimately, however, the target of the rules relating to the data protection responsibilities will – as recital 80 of the GDPR clarifies – be the controller or processor, i.e. in this case the U.S. company,[184] which in a great number of cases would not be very easy to apprehend.

B. Further Duties

In order to determine what further duties a U.S. company must comply with under the GDPR, a distinction must be made as to whether the U.S. company is acting as a "controller" or a "processor" within the meaning of the GDPR.[185]

A legal definition of the term "controller" is provided in Article 4 No. 7 GDPR. It covers any natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing. If individual natural persons are acting, it must be asked who the actions is to be attributed to – the acting person him or herself (who in that case would be the controller) or the organization for which that person works (which would then be the controller).[186] Any economic links or de facto influence which may exist would not play any role in identifying the controller. The approach that needs to be taken in this regard is not an economic, but rather a legal one. Accordingly, legally independent companies are each their own controller, even if they are affiliated with each other in a group. It follows from the definition of "controller" that the possibility of a joint controllership exists, the prerequisites for which are explained in more detail in Article 26 GDPR (see IV. B. above).

Another important actor within the framework of the GDPR is the processor.[187] Pursuant to Article 4 No. 8 GDPR, a processor is any natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller. Typical cases of processing are, for example, file destruction, support by computer centers, offers of Software as

184. European Data Protection Board, *supra* note 19, at 27.

185. For more on the term "controller," *see* Article 29 Data Protection Working Party, *supra* note 161; *see also* David Powell & Kevin Walsh, *Chaotic Rollout for European Data Privacy Regulations Raises Questions for Benefit Plan Administrators*, Benefits Brief (14 June 2018), (*available at* https://www.groom.com/wp-content/uploads/2018/06/Chaotic-Rollout-for-European-Data-Privacy-Regulations-Raises-Questions-for-Benefit-Plan-Administrators.pdf.); *see also* Houser & Voss, *supra* note 87, at 67.

186. *See also* Article 29 Data Protection Working Party, *supra* note 161, at 16.

187. Powell & Walsh, *supra* note 185.

a Service (SaaS), cloud services, etc.[188] Processing is not carried out in the case of, for example, the engagement of attorneys or the preparation of tax declarations by tax advisors. The processor must render services for the controller on the basis of a contract pursuant to Article 28 GDPR. In relation to the controller, the processor more or less functions as a "data slave" or a "puppet".[189] If the processor steps out of the framework prescribed for it, however, then it will be deemed to be a controller pursuant to Article 28(10) GDPR – with the consequence that it will be subject to all of the duties incumbent on controllers.

If U.S. companies are subject to the GDPR, then depending on whether they fall under the category of a controller or a processor they must comply with a great many duties.[190] These are described in the following.

1. Ascertaining the Lawfulness of the Processing

If the U.S. company is to be considered a controller, it will first and foremost be held responsible for the lawfulness of the processing. The central rule in European data protection law in this sense would then be that the processing of personal data is generally prohibited.[191] It may occur only if either the data subjects consent to it or another statutory criterion for permissibility applies, in particular from the definitive list in the general clauses of Articles 6 and 9 GDPR, but also under national law insofar as the GDPR explicitly grants this possibility through the various opening clauses.[192]

This "prohibition with reservation of permission", which every controller has to comply with, specifies the statutory reservation on the national level for the public sphere as a general principle of EU law,[193] which must always be complied with in cases of interference with fundamental rights. Conversely, in the non-public sphere, this prohibition with reservation of permission restricts the fundamental rights of the controller. Each individual phase of the data processing requires legitimation, and thus a data

188. *See also* the examples given in IV. A. above.

189. For more on the term "processor," see Article 29 Data Protection Working Party, *supra* note 161.

190. *See also* the overview in Abraham & Loveday, *supra* note 96, at 12; Houser & Voss, *supra* note 87, at 71.

191. *See* Houser & Voss, *supra* note 87, at 75.

192. *See* III. above in this regard.

193. ECJ Case 46/87, Hoechst AG v Commission, 1989 E.C.R. 2859, at para. 19, (*available at* http://curia.europa.eu/juris/showPdf.jsf?text=&docid=95199&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=1000316).

subject's consent which merely covers the collection and storage is not sufficient for the transfer of data. It must therefore always be carefully examined whether each intended use of personal data in every phase can be supported by a criterion for permissibility. If this is not possible, then it will be necessary to refrain from processing the personal data involved. Moreover, the overarching necessity principle applies along with the prohibition with reservation of permission, as is made particularly clear with the criteria for permissibility set out in Article 6(1) sent. 1 lit. b-f GDPR, under which the processing of personal data is permissible only if this is necessary within the scope of the respective criterion for permissibility, i.e. if no sensible or reasonable alternative exists to the manner of data processing that is being contemplated in order to achieve the desired objective.[194]

2. Information Requirements

Furthermore, the GDPR provides for comprehensive information requirements for controllers.[195] In the view of the legislature, in order for data subjects to be able to avail themselves of possible options for action, it is necessary that they know in the first place that the controller is processing personal data relating to them. Proceeding from this transparency concept which is enshrined in the transparency principle of Article 5(1)(a) GDPR, the regulators have created comprehensive information requirements for the controller.

With regard to the information to be provided to the data subjects, a distinction must be made as to whether the data are collected from the data subject, and thus they themselves are functioning as direct data sources (in which case Article 13 GDPR is to be applied), or if the data are collected not from the data subjects themselves, but from, for example, third parties or publicly accessible sources (in which case Article 14 GDPR applies). As a rule, the controller is obligated to provide the data subject with information such as its identity and contact details, the contact details of a data protection officer, where applicable, the purposes of the processing for which the personal data are intended, the legal basis for the processing, and the recipients or categories of recipients of the personal data. Generally, this information must also state the period for which the data will be stored and

194. *Kühling & Klar & Sackmann, supra* note 128, at 141.

195. Extensively discussed in Article 29 Data Protection Working Party, *Guidelines on transparency under Regulation 2016/679*, WP 260 rev.01 (2018).

explain the rights to oppose the processing to which the data subject is entitled.

How the controller fulfills this duty in practice will depend on the situation at hand. If data processing on websites is involved, the data subjects will normally be informed by way of a privacy policy. If contracts are concluded, the information may be conveyed in a separate data protection information if appropriate.

3. Other Obligations vis-à-vis Data Subjects

Articles 15 et seq. of the GDPR set out additional specific data protection rights benefitting data subjects which U.S. companies must comply with if they are subject to the GDPR as controllers.

For example, in the view of the European lawmakers it is of essential importance for data subjects to be able to learn by obtaining access to information whether the controller is processing any personal data concerning them, and if so, what personal data is involved. In fact, Article 8(2) sent. 2 of the Charter of Fundamental Rights of the European Union (CFREU)[196] directly gives rise to the right to be informed: "Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified." Against this background, the right of access upon request pursuant to Article 15 GDPR which, moreover, is also enshrined in the transparency principle of Article 5(1)(a) GDPR, is of particular importance. The data subject has the right to obtain information in particular on whether personal data are being processed by the controller and if that is the case, information on the purposes of the processing, the categories of personal data which are being processed and the recipients or categories of recipients of the data. In fact, the data subject must be provided with a copy of his or her personal data, provided that this does not adversely affect the rights of any third parties. In practice, fulfilling this right to information can result in a great expenditure of time and money. It is presumably also for this reason that it has become "fashionable" in practice to assert it in situations in which, for example, an employee would like to drive up his or her severance payment.

Article 16 sent. 1 GDPR provides the data subject with the right to obtain from the controller the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject also has the right to have incomplete personal data completed (Article 16 sent. 2 GDPR). The right to rectification upon request

196. Charter of Fundamental Rights of the European Union, 2000 O.J. C 364/1.

supplements the principle of data accuracy pursuant to Article 5(1)(d) GDPR, which obligates the controller to ensure data accuracy even if no request is made. On a primary level of EU law, the right to rectification is established in Article 8(2) sent. 2 CFREU: "Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified."

Pursuant to Article 17(1) GDPR, subject to certain conditions, the data subject additionally has the right to obtain from the controller the erasure of personal data concerning him or her without undue delay. This right is in line with the controller's corresponding duty to erase which, in a general form, already derives from the principle of storage limitation pursuant to Article 5(1)(e) GDPR. Paragraph 1 of Article 17 GDPR is structured as a classical right to erasure, which is supplemented in paragraph 2 with special information requirements (in the sense of the right to be forgotten).[197] The obligation to erase generally applies in the cases mentioned in Article 17(1) GDPR independently of a request by the data subjects.[198] This means as a rule that companies have to define erasure dates for their various processing activities and record them in an archiving and erasure concept.

Subject to certain conditions, a data subject has the right under Article 18 GDPR to demand that the controller restrict the processing of personal data concerning him or her. What is meant here is the blocking of personal data. This term is described in Article 4 No. 3 GDPR as the marking of stored personal data with the aim of limiting their processing in the future. As a rule, this restriction serves to achieve a (temporary) balance between the data subject's interest in protection and the controller's interest in processing the data.[199]

Article 20 GDPR grants the data subject a right against the controller to data portability upon request.[200] This right, which provides data subjects with a comprehensive power to dispose of "their" data, was newly created in the

197. For a criticism of the term, see Houser & Voss, *supra* note 87, at 72.

198. *Kühling & Klar & Sackmann, supra* note 128, at 250.

199. In general, *on the right to be forgotten in the Internet,* Meg Leta Ambrose, *A Digital Dark Age and the Right to Be Forgotten*, 17 J. INTERNET L. 8, 9 (2013); Bennett, *supra* note 97, at 167; Ryan Budish, *In The Face of Danger: Facial Recognition and the Limits of Privacy Law*, HARV. L. REV. 1870, 1874 (2007); Francoise Gilbert, *The Right of Erasure or Right to Be Forgotten: What the Recent Laws, Cases, and Guidelines Mean for Global Companies*, 18 J. INTERNET L. 14, 15 (2015); Benjamin J. Keele, *Privacy by Deletion: The Need for a Global Data Deletion Principle*, 16 IND. J. GLOBAL LEGAL STUD. 363, 375 (2009); Emily Adams Shoor, *Narrowing the Right to be Forgotten: Why the European Union Needs to Amend the Proposed Data Protection Regulation*, 39 BROOK. J. INT'L L. 487, 517 (2014); Mark Tunick, *Privacy and Punishment*, 39 SOCIAL THEORY AND PRACTICE 643, 667 (2013).

200. *See also* Houser & Voss, *supra* note 87, at 74.

GDPR. There was no model for it in European law up to that point. It is closely related to the right of access, but differs from it in many ways.[201] The right to data portability – like the right to information – is meant to ensure that the data subject can further strengthen the control over his or her own data (see recital 68 of the GDPR[202]). At the same time, it should be possible and as uncomplicated as possible for a data subject to switch from one controller to a different one,[203] which may provide more data protection-friendly systems. In this respect, the provision is also pursuing competition policy objectives. At the same time, it contributes to the development and use of interoperable formats. Furthermore, the right to data portability will reduce any "lock-in effects" (with antitrust implications) which may exist,[204] and could particularly play a role with regard to internet service providers. Accordingly, the discussion on creating a right to data portability focused primarily on social networks. But the provision is also applicable beyond that, for example in connection with music streaming services, webmail applications,[205] banks or insurances. In its content, the right to data portability covers both the data subjects' right to obtain all or part of the personal data concerning them which they had provided to the controller[206] and to have the controller transfer these data to another controller.[207] However, the other controller is not obligated to take receipt of the data. The data subject may also directly demand that the controller transmit the relevant personal data to another controller, where technically feasible.[208] The transmission to the second controller should then be carried out "without hindrance" from the first controller under the provision. Hence, any technical or legal hindrance, as well as any delay in execution, must be avoided. In

201. Article 29 Data Protection Working Party, *Guidelines on the right to data portability*, WP 242 rev.01, 3 (2017).

202. Recital 68 of the GDPR: "To further strengthen the control over his or her own data, where the processing of personal data is carried out by automated means, the data subject should also be allowed to receive personal data concerning him or her which he or she has provided to a controller in a structured, commonly used, machine-readable and interoperable format, and to transmit it to another controller."

203. Article 29 Data Protection Working Party, *supra* note 201, at 3.

204. *See* Article 29 Data Protection Working Party, *supra* note 201, at 5.

205. Article 29 Data Protection Working Party, *supra* note 201, at 5.

206. On the right to data portability in the case of complex data structures, see Article 29 Data Protection Working Party, *supra* note 201, at 18.

207. Article 20(1) GDPR.

208. Article 20(2) GDPR.

this respect, when transmitting the data, the controller is acting on behalf of the data subject.[209]

Pursuant to Article 21 GDPR, in certain situations the data subject has the right to object to the processing of personal data affecting him or her by a controller, thus ensuring that the controller will no longer be allowed to process the data involved. The provision defines various situations in which the data subject can object to the processing. What they all have in common is that the right to object is directed at processing which is lawful in and of itself but is not in line with the intention of the data subject. The right to object under Article 21 GDPR is not to be confused with a data subject's right to withdraw his or her consent under Article 7(3) sent. 1 GDPR, which pertains to a consent that had been given by the data subject.

Moreover, pursuant to Article 77 GDPR, the data subject is free to lodge a complaint with a supervisory authority if he or she considers that the processing of the personal data relating to him or her infringes the GDPR. Additionally, the data subject has the right to a judicial remedy against a supervisory authority in accordance with Article 78 GDPR or against the controller or processor pursuant to Article 79 GDPR. Finally, Article 82(1) GDPR regulates compensation claims against the controller or the processor due to infringements of the GDPR, as a result of which the data subject suffered material or non-material damage.

4. Designation of a Data Protection Officer

Subject to the prerequisites set out in Article 37 GDPR, U.S. companies must designate an (internal or external) data protection officer.[210] The requirements placed on the duty to designate a data privacy officer are regulated in Article 37 GDPR.[211] Consequently, U.S. companies within the scope of the GDPR will have to designate a data protection officer if their core activities, i.e., the most important work processes which are necessary to achieve their objectives, consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale[212] or their core

209. On the responsibility in these cases, see Article 29 Data Protection Working Party, *supra* note 201, at 6.

210. *See also* Houser & Voss, *supra* note 87, at 77.

211. *See also* the more detailed explanations in Article 29 Data Protection Working Party, *Guidelines on Data Protection Officers ('DPOs')*, WP 243 rev.01 (2017).

212. *See* Article 37(1)(b) GDPR.

activities consist of processing on a large scale of special categories of data (concerning health, genetic data, etc.).[213]

If a data protection officer is to be designated, his or her main task is to work to ensure that the controller complies with the legal data protection rules and to inform and advise it with regard to data protection issues.[214] He or she must further cooperate with the data protection supervisory authority for which he or she is the central contact point at the controller or processor.[215] Data subjects may also contact the data protection officer, who must assist and advise them.[216]

5. Documentation Duties

One substantive change to the GDPR is the far more stringent documentation duties which can definitely create a burden for companies in practice. Of central importance in this regard is the provision in Article 5(2) GDPR that the controller is not only responsible for the lawfulness of the data processing, but must consistently be able to demonstrate it (accountability). In practice, this can only be achieved by way of complete documentation. This requirement serves several functions; the duty to provide documentation has a reflexive effect on the controller itself, which should take this occasion to become aware of the extent of its processing activities and their lawfulness. For this reason, a violation of the documentation duties themselves is subject to a fine.[217] It is therefore a function of self-monitoring which is similar to the warning function of a formal requirement under civil law. Moreover, well-managed documentation facilitates the fulfillment of requests for information by the supervisory authorities. Last, but not least, this also reverses the burden of proof, putting the data subject who seeks to take action against unlawful data processing in a stronger position.

Specifically, the GDPR in particular provides for general accountability under Article 5(2) GDPR in conjunction with Article 24(1) GDPR, as well as a duty to maintain a record of processing activities ("processing record") pursuant to Article 30 GDPR.[218] A violation of this duty is subject to a fine.

213. *See* Article 37(1)(c) GDPR.

214. *See* Article 39(1)(a) GDPR.

215. Article 39(1)(d) and (e) GDPR.

216. Article 38(4) GDPR.

217. Article 83(4)(a) GDPR.

218. Article 5(2) GDPR: "The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')." Article 24(1) GDPR: "Taking into account the nature, scope, context and purposes of processing as well as the risks of

The processing record must contain the information listed in Article 30(1) GDPR, such as the name and the contact details of the controller, the purpose of the processing, a description of the categories of data subjects, etc. Processors must also maintain a record with a similar content.[219]

6. Notification Duties

Controllers are additionally obliged to notify data protection breaches to the competent supervisory authority without undue delay.[220] In the case of U.S. companies who offer goods or services to persons in the European Union or monitor their behavior, several data protection authorities in the European Union may have parallel competence in this regard.[221] Data protection breaches are legally defined in Article 4 No. 12 GDPR as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed. Thus, this is directed at the classical "data protection failures," which are often caused by IT security defects. The purpose of the notification duty is so that the supervisory authorities can be involved early on and assist the controller in handling the problem. However, a notification is not necessary if the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. The controller must assess this question on its own responsibility in a predictive decision taking into consideration the severity of the possible consequences and the likelihood that they will occur.[222] The notification must be drawn up by the controller. If a processor becomes aware of a data protection breach, it must inform the controller thereof without undue delay.[223] Such a duty also derives from the mandatory commissioned data processing agreement.[224]

The controller must submit the notification without undue delay and, where feasible, no later than 72 hours after having become aware of it. The

varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary."

219. *See* Article 30(2) GDPR.

220. *See* Article 33 GDPR. For more information, see Article 29 Data Protection Working Party, *Guidelines on Personal data breach notification under Regulation 2016/679*, WP 250 rev.01 (2018).

221. *See* recital 122 sentence 2 of the GDPR.

222. Article 29 Data Protection Working Party, *supra* note 220, at 8.

223. Article 33(2) GDPR.

224. *See* Article 28(3) sent. 2 lit. f GDPR.

controller must in particular describe the nature of the breach, including where possible the categories and approximate number of persons concerned and the categories and approximate number of personal data records concerned, as well as the likely consequences of the personal data breach and the measures taken or proposed to be taken by the controller.[225] This is to enable the supervisory authority to quickly obtain an overview of the extent and consult on its response.

In the event of a personal data breach, the controller must not only inform the supervisory authority, but also, under certain circumstances, the data subjects as well (Article 34 GDPR). This is necessary if the breach is likely to result in a high risk to the rights and freedoms of natural persons. The system involved is the reverse of that for the duty to notify the supervisory authority: the communication is not necessary as a rule, but only in exceptional cases if the breach is likely to result in a high risk to the rights and freedoms of natural persons. However, the communication will not be required if, for example, the relevant data are protected by technical and organizational protection measures (such as effective encryption),[226] due to countermeasures taken by the controller, the high risk to the rights and freedoms of data subjects is no longer likely to materialize[227] or the communication would involve disproportionate effort to carry out.[228] In the latter case, individual communications would be replaced by a public communication or similar measure in a form which will make it possible for the data subjects to obtain knowledge of the breach. This could be accomplished primarily through daily newspapers or publications on the internet. If the controller fails to comply with this duty it can also be ordered to do so by a supervisory authority.[229] Moreover, a breach of the duty to communicate is subject to a fine.[230]

7. Data Protection Impact Assessment

Under Article 35 GDPR, it is mandatory for certain processing operations that the controller carry out a data protection impact assessment. The purpose of this is for the controller in particularly sensitive areas to be

225. Article 33(3) GDPR.
226. Article 34(3)(a) GDPR.
227. *See* Article 34(3)(b) GDPR.
228. Article 34(3)(c) GDPR.
229. *See* Article 34(4) GDPR.
230. Article 83(4)(a) GDPR.

aware of the possible consequences of the data processing operations by means of a structured procedure.[231]

According to the statutory provisions, a data protection impact assessment must always be carried out where the type of processing, in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons.[232] In that case, the controller must first assess the impact of the envisaged processing operations on the protection of personal data. The GDPR provides some examples of when a data protection impact assessment must be carried out.[233] For example, a data protection impact assessment is required in the case of a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person.[234] A data protection impact assessment is also required in the case of processing on a large scale of special categories of data or of personal data relating to criminal convictions and offences.[235] Moreover, a data protection impact assessment is required in the case of a systematic monitoring of a publicly accessible area on a large scale.[236] The Article 29 Data Protection Working Party formulated additional scenarios in its Working Paper 248 in which a data protection impact assessment would be necessary.[237]

VI. Conclusion

With the help of an expanded territorial scope of the European data protection law, the European legislature is striving to protect the privacy rights of data subjects in the European Union comprehensively and worldwide. Since American privacy concepts clearly differ from the understanding traditionally found in Europe,[238] the extraterritorial effect of

231. *See* Article 29 Data Protection Working Party, *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679*, WP 248 rev.01 (2017).

232. Article 35(1) GDPR.

233. *See* Article 35(3) GDPR.

234. Article 35(3)(a) GDPR.

235. *See* Article 35(3)(b) GDPR.

236. Article 35(3)(c) GDPR.

237. For more on this, see Article 29 Data Protection Working Party, *supra* note 231.

238. *See* Klar & Kühling, *supra* note, at 98; Paul M. Schwartz & Karl-Nikolaus Peifer, *Transatlantic Data Privacy Law*, 106 GEO. L.J. 115 (2017).

the GDPR is likely to have an explosive impact on the relationship between these U.S. and European approaches to privacy. The offering of U.S. products and services in Europe is caught up in one blow and legally fed into the regulation by European institutions. In view of the broad (territorial) scope of the GDPR and its enhanced clout as a harmonizing regulation, European data protection law will once again gain more influence on the general data protection conditions of worldwide trade.[239] This effect is strengthened by the fact that even if the provisions of the GDPR are not directly applicable for U.S. companies, they are often contractually obliged by their European partners to comply with a data protection standard similar to that of the GDPR. However, one should not lose sight of the fact that U.S. companies which are bound by the rules of the GDPR also have to comply at the same time with the national data protection requirements under U.S. law, as well as possibly those of other jurisdictions. This fact should be taken into account with an appropriately restrictive interpretation of the scope of the GDPR and its requirements imposed on data controllers outside the EU.

In the US, the strong influence exerted by California's comparatively high data protection standards on the other states is known as the "California effect."[240] With regard to the GDPR, it is becoming apparent that the extraterritorial approach of European data protection is leading to a "Brussels effect" worldwide.[241] Given the expansion of the scope of European data protection law, U.S. companies should at least obtain an overview of the new provisions and ascertain whether or not the GDPR is applicable to them. It would also make sense to delve more deeply into this issue, since it can be assumed that more states will be sharpening up their data protection rules or adapting themselves to the high standard which the GDPR is setting beyond any doubt.

239. Making reference to this "ratcheting-up" effect: Marc Rotenberg & David Jacobs, *Updating the Law of Information Privacy: The New Framework of the European Union*, 36 HARV. J.L. & PUB. POL'Y 605, 636 (2013); *see also* Gömann, *supra* note 9, at 568; critical: Svantesson, *supra* note 9, at para. 28; critical from an international law perspective: Azzi, *supra* note 2, at 130, as well as Wimmer, *supra* note 8, at 557.

240. *See* Bradford, *The Brussels Effect*, 107 NW. U. L. REV. 1, 22 (2012).

241. *See also* Bradford, *supra* note 240, at 22.