Stanford – Vienna
Transatlantic Technology Law Forum

A joint initiative of
Stanford Law School and the University of Vienna School of Law

TTLF Working Papers

No. 20

The New General Data Protection Regulation of the EU and its Impact on IT Companies in the U.S.

Anna Zeiter

2014

TTLF Working Papers

About the TTLF Working Papers

TTLF's Working Paper Series presents original research on technology, and business-related law and policy issues of the European Union and the US. The objective of TTLF's Working Paper Series is to share "work in progress". The authors of the papers are solely responsible for the content of their contributions and may use the citation standards of their home country. The TTLF Working Papers can be found at http://ttlf.stanford.edu. Please also visit this website to learn more about TTLF's mission and activities.

If you should have any questions regarding the TTLF's Working Paper Series, please contact Vienna Law Professor Siegfried Fina, Stanford Law Professor Mark Lemley or Stanford LST Executive Director Roland Vogl at the

Stanford-Vienna Transatlantic Technology Law Forum
http://ttlf.stanford.edu

Stanford Law School
Crown Quadrangle
559 Nathan Abbott Way
Stanford, CA 94305-8610

University of Vienna School of Law
Department of Business Law
Schottenbastei 10-16
1010 Vienna, Austria

About the Author

Anna Zeiter is the Head of Data Protection for eBay Marketplaces in the European Union. Before joining eBay Anna Zeiter graduated in 2014 with honors from the LL.M. Program in Law, Science & Technology at Stanford Law School. From 2009 until 2013 Anna has been working as a lawyer for two international law firms in Hamburg (DLA Piper and Norton Rose Fulbright), specializing in data protection, IT and ecommerce law. Before working as an attorney Anna Zeiter studied law, music and art history in Osnabruck and Florence. After that she did her Ph.D. in the field of free speech and media law at the University of Hamburg. During that time she worked as a research assistant at the Hans-Bredow Institute for Media Research at the University of Hamburg. Anna gives regular presentations and lectures on data protection and IT law issues, and the compliant implementation of ecommerce business models. In addition to that, Anna has published during the past years various papers and articles on data protection, IT and ecommerce law.

General Note about the Content

Suggested Citation

This TTLF Working Paper should be cited as:
Anna Zeiter, The New General Data Protection Regulation of the EU and its Impact on IT Companies in the U.S., Stanford-Vienna TTLF Working Paper No. 20, http://ttlf.stanford.edu.

Copyright

Abstract

The European Commission intends to unify data protection within the European Union (EU) with a single law, the General Data Protection Regulation (GDPR). The background is that the current EU Data Protection Directive 95/46/EC of 1995 does not sufficiently take into account important developments like globalization and technological advancements such as social networks and cloud computing. Therefore, the European Commission published in January 2012 a comprehensive draft legislation to establish a unified European data protection law within the EU. In March this year the European Parliament voted in favor for the adoption of the GDPR. The bill now moves to the European Council of Ministers for potential further amendments. The European Parliament's aim is to reach an agreement with the European Council of Ministers before the end of 2014. The proposed GDPR will not only bring advantages but also additional data protection obligations to IT companies in the U.S. On the one hand, the different data protection laws across the 28 Member States will be harmonized which will make the business of multinational U.S. companies in the EU much easier. Additionally, the proposed one-stop-shop system will make it simpler and cheaper for global IT companies to do business in the EU because in the future such companies will only have to deal with one responsible DPA. However, on the other hand, the current version of the GDPR also includes new data subjects' rights like the right to erasure, the right to access and obtain data as well as the principle of data protection by design and by default. According to the new regulation, these data subjects' rights will also apply to U.S. companies without any establishment in the EU, as long as they process personal data of EU residents. Against this background, IT companies in the U.S. have to be attentive and should start preparing now for this fundamental change in the European data protection landscape.

Table of Contents

I. Introduction

The European Commission plans to unify and strengthen data protection within the (EU) with a single law, the General Data Protection Regulation (GDPR).

The following is the background of this legislative project. The current Data Protection Directive in the EU[1] does not sufficiently take into account the widespread use of the Internet and important developments like globalization and technological advancements like social networks and cloud computing. Accordingly, the European Parliament determined that new guidelines for

[1] 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) ("Data Protection Directive").

data protection were required.[2] Additionally, the current Data Protection Directive grants the 28 Member States broad discretion in the implementation of minimal standards. The result is that the current data protection situation in the EU is a patchwork of 28 different data protection regimes which has created unequal data protection levels and legal uncertainty.[3]

Therefore, the European Commission unveiled on 25 January 2012 a comprehensive draft legislation to establish a unified European data protection law within the EU.[4] This includes, in particular, a draft of the GDPR that will have a direct and binding effect on all 28 EU Member States by replacing the patchwork of different data protection laws currently in force. In addition, it is also aim of the European Commission – while still relying on the basic ideas of the Data Protection Directive[5] – to strengthen with the introduction of the GDPR the rights of the data subjects, give consumers greater control over their personal data, introduce stricter sanctions for data protection breaches and make the new data protection law also applicable to foreign companies handling the data of EU residents.[6]

After publication of the European Commission's draft regulation in January 2012 almost 4,000 amendments have been proposed to the GDPR by different committees of the European

---

[2] Eur. Parl., *Q&A on EU data protection reform* (Mar. 4, 2014), http://www.europarl.europa.eu/news/de/news-room/content/20130502BKG07917/html/QA-on-EU-data-protection-reform; Eur. Parl. Civil Liberties, Justice and Home Affairs Committee (LIBE), Inofficial Consolidated Version After LIBE Committee Vote Provided By The Rapporteur, Regulation Of The European Parliament And 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 – Consolidated Version of LIBE), Recitals (5), (9) (Oct. 22, 2013).

[3] 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, 68 (2014); Lukas Feiler, INFORMATION SECURITY LAW IN THE EU AND THE U.S., 2012, at 109.

[4] Eur. Comm'n, *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 free movement of such data*, EUR. COMM'N DOC. (COM (2012) 11 final, Jan. 25, 2012) (General Data Protection Regulation – Initial Version of European Commission).

[5] General Data Protection Regulation – Consolidated Version of LIBE, Recital (7); Andrej Savin, EU INTERNET LAW 206 (2013).

[6] Press Release, Eur. Comm'n, Progress on EU data protection reform now irreversible following European Parliament vote (Mar. 12, 2014) (on file with author); Eur. Parl., *Q&A on EU data protection reform* (Mar. 4, 2014) http://www.europarl.europa.eu/news/de/news-room/content/20130502BKG07917/html/QA-on-EU-data-protection-reform.

Parliament and the European Council of Ministers.[7] While working on these amendments as well as dealing with the numerous studies, debates and comprehensive lobbying from all conceivable sides over the last two years, it became unclear if the European Parliament will decide on the GDPR during this legislative period.

However, very recently, on 12 March 2014, the European Parliament voted in plenary on first reading with 621 of 653 votes in favor for the adoption of a consolidated version of the GDPR[8] which was provided by the European Parliament's Civil Liberties, Justice and Home Affairs Committee (LIBE) and its rapporteur, Jan-Philipp Albrecht, in October 2013.[9] This version of the GDPR is now the binding basis for further legislative procedures.[10] Under EU legislative rules, the bill now moves to the European Council of Ministers, roughly equivalent to the upper parliamentary chamber consisting of Member State government representatives.[11] There, the proposal will be subject to potential further amendments. However, the vote of 12 March 2014 requires the new European Parliament, which will reconstitute in July 2014 after the forthcoming elections in May 2014, to take over the work done by the European Parliament in its current term. That means that after 12 March 2014 it is clear that the GDPR will be enacted in any form whatsoever.

Although the legislative process in the EU is generally known for its tardiness, it is the European Parliament's aim to reach an agreement with the European Council of Ministers on this major

[7] dataguidance.com, *Discussions on the Regulation are mature* (Jan. 30, 2014), http://www.dataguidance.com/ dataguidance_ privacy_this_week.asp?id=2197.
[8] Press Release, Eur. Comm'n,, Progress on EU data protection reform now irreversible following European Parliament vote (Mar. 12, 2014) (on file with author).
[9] General Data Protection Regulation – Consolidated Version of LIBE.
[10] Press Release, Eur.Comm'n., Progress on EU data protection reform now irreversible following European Parliament vote (Mar. 12, 2014) (on file with author).
[11] *Id*.

legislative reform before the end of 2014.[12] After enactment it is expected that the GDPR will still have a transitional period of two years. However, the clock for companies affected by this new regulation is already ticking.

Against the background of this proposed EU data protection regulation, the aim of the present paper is to explore the impact of the GDPR, with special emphasis on IT companies in the U.S. such as social networks, email and cloud service providers, search engine companies, e-commerce platforms, hardware manufacturers, and software producers. From today's perspective the new data protection regulation will especially affect data-driven companies in the IT field not only within the EU but also abroad, e.g. in the U.S., in the case of companies that handle personal data of EU residents. Therefore, this article focuses especially on those provisions of the proposed new EU regulation which will mainly affect IT companies in the U.S., such as Facebook, Google, Yahoo, eBay, Amazon, Microsoft, Dropbox, etc.

In this context the present paper will first discuss some of the relevant general provisions of the planned GDPR, such as the planned harmonization of the data protection regime within the EU, the applicability of the proposed new law to U.S. companies, the requirement to appoint a data protection officer in the EU, the data breach notification obligations, the planned one-stop-shop principle and the planned harsh sanction regime (*see infra* Part II).[13] After that, the paper will further focus on some selected rights which are of special interest for IT companies, such as the right to erasure, the right to access and to obtain data for the data subject, as well as the new requirements for data protection by design and by default (*see infra* Part III). In the conclusion,

[12] Eur. Parl., *Q&A on EU data protection reform*, http://www.europarl.europa.eu/news/de/news-room/content/20130502BKG07917/html/QA-on-EU-data-protection-reform (Mar. 4, 2014).
[13] This article especially does not discuss the provisions of the proposed GDPR on consents, profiling, international data transfers, and law enforcement.

this paper will summarize the legal impact as well as provide an overview of the impact the GDPR will have especially on U.S. IT companies from a business perspective (*see infra* Part IV).

II. General Provisions

A. Harmonization of Data Protection Laws within the EU

The main change of the GDPR is that it will harmonize data protection law throughout the entire EU. That means in the future only a single set of rules on data protection will be valid across all 28 Member States, replacing the current inconsistent patchwork of national data protection laws ("one continent – one law").[14]

Although the current Data Protection Directive already provides a legislative framework, the data protection situation in the EU is still a mosaic of 28 different data protection regimes. The reason for that is that under EU law, directives usually set a common aim but leave it to each of the Member States to choose the form and the methods by which the directive is implemented in national law.[15] For this reason, directives like the current Data Protection Directive can be adopted by means of a variety of legislative procedures depending on their subject matter. Therefore, currently in the EU 28 slightly different national data protection laws exist under the framework of the Data Protection Directive.[16]

[14] Press Release, Eur.Comm'n., Progress on EU data protection reform now irreversible following European Parliament vote (Mar. 12, 2014) (on file with author).
[15] Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union – Consolidated version of the Treaty on the Functioning of the European Union – Protocols – Annexes – Declarations annexed to the Final Act of the Intergovernmental Conference which adopted the Treaty of Lisbon, signed on Dec. 13, 2007 – Tables of equivalences (Treaty on the Functioning of the European Union – TFEU), Article 288 Section 3 2012 O.J. (C 326, Oct. 26, 2012 P. 0001 0390) ("TFEU"); 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, 68 (2014).
[16] Lukas Feiler, INFORMATION SECURITY LAW IN THE EU AND THE U.S. 109 (2012).

In contrast to that, regulations like the proposed GDPR are legal acts of the EU that become immediately and simultaneously enforceable as law in all Member States.[17] That means that when the GDPR is in force by the end of 2014, only one single set of data protection rules will be in force in the EU, and the current data protection legislations in the Member States as well as the Data Protection Directive will not be applicable anymore.[18] In addition, the Member States will not be able to change or weaken the GDPR afterwards through national laws. However, with this new regulation full harmonization in the data protection sector will *de facto* not be achieved. The current version of the GDPR contains *inter alia* exceptions for health and employee data that still might be, to a certain extent, subject to individual country regulations.[19]

This huge legislative change – the harmonization of data protection law across all 28 Member States – will make the businesses of multinational companies in the EU generally much easier. Such companies only have to comply with a single set of data protection rules (and not with 28 different data protection laws) when they offer products or services to customers based in the EU.[20] Against this background, international companies like social networks, search engine providers, e-commerce companies and cloud computing businesses are explicitly welcoming the idea of a single data privacy law stretched across the EU. From this perspective, the proposed GDPR will reduce the costs of the companies' compliance activities. The benefits of a harmonized EU data protection law are estimated by the European Commission confidently at 2.3 billion EUR per year.[21] However, the remaining fragmentation for health and employee data at

[17] TFEU Article 288 Section 2; 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, 68 (2014).
[18] However, European Commission's decisions adopted and authorizations by supervisory authorities based on the Data Protection Directive should remain in force. *See* General Data Protection Regulation – Consolidated Version of LIBE, Recital (134).
[19] General Data Protection Regulation – Consolidated Version of LIBE, Recital (124), Article 81 and 82.
[20] Press Release, Eur.Comm'n., Progress on EU data protection reform now irreversible following European Parliament vote (Mar. 12, 2014) (on file with author).
[21] *Id*.

the domestic level will still be a burden for companies, especially for cloud computing services and providers of Enterprise Resource Planning (ERP) systems, which are hosting and processing employee data from many different EU Member States.

B. Applicability to Non-EU-Companies

Besides that, the planned GDPR will extend the territorial scope of the EU data protection law explicitly to all organizations that process personal data of EU residents. That means in the future EU-foreign companies fall under the regulation if they process personal data of subjects residing in the EU ("the same rules for all companies – inside and outside the EU").[22]

In contrast to that, the current law in the EU is not so far reaching: According to Article 4.1. the of the Data Protection Directive national data protection laws are applicable if "(a) the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State … (c) the controller is not established on Community territory and, for purposes of processing personal data makes use of equipment … situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community." That means the current Data Protection Directive claims jurisdiction over foreign data controllers only when the controller "has an establishment" in the EU or "makes use of equipment" which is situated in the EU (except for transitory purposes).[23] However, in absence of a definition[24], the term "equipment" in this provision is interpreted generally very broadly and may in some cases even result in EU data protection law being

[22] *Id. See also* 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, 53 ff. (2014).
[23] Andrej Savin, EU INTERNET LAW 197 (2013).
[24] 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, 65 (2014).

applicable where the processing in question has no real connection with the EU.[25] This leads currently to situations where EU data protection law applies to controllers who have no connection with the EU other than the fact that they use or rent equipment physically located in the EU.[26] On the other hand this results in situations where EU data protection law does not apply to controllers outside the EU who deal exclusively or largely with EU customers and have no processing equipment located in the EU.[27] In sum, the current provision in the Data Protection Directive which deals with its applicability is quite complex, unclear and confusing.[28]

The applicability provision of the proposed GDPR is, in contrast, not only clearer but also broader:[29] According to Article 3.2. of the current version of the GDPR the new regulation explicitly "applies to the processing of personal data of data subjects 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 such data subjects."

That means that contrary to the current Data Protection Directive, the GDPR will apply without ambiguity to all organizations based outside the EU, e.g. companies based in the U.S., without any establishment in the EU only if they process personal data[30] of EU residents.[31] That means

[25] Article 29 Data Protection Working Party, Opinion 8/2010 on applicable law (WP 179) (Dec. 16, 2010); *see also* Lukas Feiler, INFORMATION SECURITY LAW IN THE EU AND THE U.S. 109 (2012).
[26] Andrej Savin, EU INTERNET LAW 197 (2013).
[27] *Id*.
[28] *See also* 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, 65, 73, 100 (2014).
[29] Andrej Savin, EU INTERNET LAW 206 (2013).
[30] In comparison to the U.S. also the EU definition of "personal data" is relatively broad. According to the Article 29 Data Protection Working Party, "personal data" is any information relating to an identified or identifiable natural person. This can be anything from a name, a photo, an email address, bank details, posts on social network websites, medical information, or even computer's IP address. *See also* Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data (WP 136) (Jun. 20, 2007).
[31] General Data Protection Regulation – Consolidated Version of LIBE, Recitals (19), (20); 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).

that any U.S. company that processes personal information of EU residents (e.g. by providing contractual services to EU residents from abroad or even tracking the behavior of EU residents on their non-EU websites) is required to abide by the proposed EU data protection law.[32] As a result, all U.S. websites, search engines, social networks, e-commerce platforms, cloud services and apps available in the EU are covered in the future by the new regulation.[33] Thus, not only IT companies or data-driven companies, but also every U.S. business with a simple online presence is at risk of being exposed to the new EU's strict data protection laws.[34] Additionally, companies which happened to sell something or provide online services to customers in the EU even on a one-off basis will have to comply with the entire GDPR.[35] Therefore, Article 3.2. of the current version of the GDPR will significantly extend the scope of EU law to include U.S. companies with no physical presence or assets in the EU.[36] It is certainly no exaggeration to state that for any non-EU company Article 3.2. of the current GDPR is probably the most important provision of the entire proposed regulation.[37]

In practice this new provision represents a huge change. The GDPR will not only affect foreign companies with customers or users, but also those with business partners and employees residing in the EU. Therefore, this main provision of the new EU data protection law may force U.S. companies in the near future to not only comply with EU data protection law in all aspects but

[32] Dan Jerker B. Svantesson, *How Europe's data privacy reform could cost Australian business*, theconversation.com (Mar. 12, 2014), https://theconversation.com/how-europes-data-privacy-reform-could-cost-australian-business-24210.
[33] 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, 74 (2014).
[34] *Id*. at 74.
[35] *Id*. at 73; Dan Jerker B. Svantesson, *How Europe's data privacy reform could cost Australian business*, theconversation.com (Mar. 12, 2014), https://theconversation.com/ how-europes-data-privacy-reform-could-cost-australian-business-24210.
[36] 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, 75 (2014).
[37] *Id*. at 71.

also establish European data protection management, e.g. by appointing a European data protection officer.[38]

C. Appointment of a Data Protection Officer

As mentioned, the proposed GDPR contains another huge obligation: the new law requires companies to appoint a Data Protection Officer (DPO) in the EU. That means that foreign companies without any establishment in the EU, but which are handling personal data of EU residents, will have to fulfill this organizational duty.

The requirement to appoint a DPO for a company is generally new to EU data protection law. Currently the Data Protection Directive does not impose such an obligation. However, in Germany, for example, the requirement to appoint a company DPO already exists in national data protection law. This provision was actually the basis for the GDPR proposal.[39]

Article 35.1 of the current version of the GDPR states:

> The controller and the processor shall designate a data protection officer in any case where: … (b) the processing … relates to more than 5000 data subjects in any consecutive 12-months period or (c) the core activities of the controller or processor consist of processing operations which … require regular and systematic monitoring of data subjects; or (d) the core activities of the controller or processor consist of processing special categories of data …, location data or data on children or employees in large scale filing systems.

[38] *See infra* under Section II. 3. Data Protection Officers.

[39] Bundesdatenschutzgesetz [BDSG] [Federal Data Protection Act], Dec. 20, 1990, Bundesgesetzblatt [BGBl.] I S. 2954, as amended, § 4f (Ger.); Eur. Parl., *Q&A on EU data protection reform* (Mar. 4, 2014), http://www.europarl.europa.eu/news/de/news-room/content/20130502BKG07917/html/QA-on-EU-data-protection-reform; Susanne Dehmel & Nils Hullen, *Auf dem Weg zu einem zukunftsfähigen Datenschutz in Europa? Konkrete Auswirkungen der DS-GVO auf Wirtschaft, Unternehmen und Verbraucher*, 3 ZD 147, 152 (2013).

However, the position as DPO cannot be held by any employee – it requires specific expert knowledge.[40] According to Article 35.5, "The controller or processor shall designate the data protection officer on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and ability to fulfill the tasks referred to in Article 37".

Article 36 goes on to describe the position of the DPO in the company. It states:

> 1. The controller or the processor shall ensure that the data protection officer is properly and in a timely manner involved in all issues which relate to the protection of personal data. 2. The controller or processor shall ensure that the data protection officer performs the duties and tasks independently and does not receive any instructions as regards the exercise of the function. The data protection officer shall directly report to the executive management of the controller or the processor.… 3. The controller or processor shall support the data protection officer in performing the tasks and shall provide all means, including staff, premises, equipment and any other resources necessary to carry out the duties referred to in Article 37, and to maintain his or her knowledge.

Article 37.1 sets out the specific tasks of a DPO. It states:

> The controller or processor shall entrust the data protection officer at least with the following tasks: (a) to raise awareness, to inform and advise the controller or the processor of their obligations pursuant to this Regulation, …; (b) to monitor the implementation and application of the policies of the controller or processor in relation to the protection of personal data, … the training of staff …, and the

[40] General Data Protection Regulation – Consolidated Version of LIBE, Recital (75a).

> related audits: (c) to monitor the implementation and application of this Regulation …; (e) to monitor the documentation, notification and communication of personal data breaches …; (h) to act as the contact point for the supervisory authority ….

That means that in the future not only EU companies but also foreign companies, like U.S. companies which handle personal data of more than 5,000 EU residents within 12 months, or companies which are carrying out particularly intense data processing, have to appoint a company DPO in the EU. In addition, such a DPO has to be an expert with in-depth knowledge of data protection law.[41] That means that he or she should have at least the following qualifications: extensive knowledge of the substance and application of data protection law, including technical and organizational measures and procedures, mastery of technical requirements for privacy by design and by default[42] as well as data security, industry-specific knowledge in accordance with the size of the company and the sensitivity of the data to be processed, the ability to carry out inspections, consultations, documentations, and log-file analysis, and the ability to work with employee representation.[43] Besides that, the company has to guarantee that the DPO holds a specific position within the company which allows him or her to fulfill the described tasks with the necessary due diligence and independence and protects the DPO against dismissal.[44] However, the final responsibility for data protection decisions shall still remain with the management of the company.[45]

In sum, this new requirement will impose a harsh administrative and also be a substantial financial burden for companies, especially for U.S. companies which do not have any business

[41] *Id*. Recital (75a).
[42] *See infra* under Section III. 3. Data Protection by Design and by Default.
[43] General Data Protection Regulation – Consolidated Version of LIBE, Recital (75a).
[44] *Id*. Recital (75).
[45] *Id*.

premises in the EU. They have to implement potentially costly measures to appoint a DPO in the EU.[46] However, according to the rapporteur of the European Parliament's Civil Liberties, Justice and Home Affairs Committee (LIBE), Jan Philipp Albrecht, for foreign companies without any business premises within the EU, it will also be possible to appoint an external DPO on a per hour basis,[47] e.g. a lawyer or law firm based in the EU.

Since the DPO is appointed, according to Article 35.7 of the current version of the GDPR, for at least four years (in the case of employees) and at least two years (in case of external contractors), and because the DPO is protected against dismissal, organizations will have to consider very carefully who to appoint. As mentioned above, the tasks of the DPO are broad-ranging and comprise *inter alia* the duty to inform and advise the data controller or data processor of its obligations to monitor the implementation and application of data protection policies, to monitor the documentation, notification and communication of personal data, and to respond to requests from data subjects or the Data Protection Authority (DPA).[48] Against this background, the company also has to ensure that the DPO is practically involved in all issues that relate to the protection of personal data and maintain detailed documentation on all processing operations.[49] This will require, besides the new position of a DPO, also new processes as well as new communication channels within the company. However, on the positive side, if a DPO is

[46] Dan Jerker B. Svantesson, *How Europe's data privacy reform could cost Australian business*, theconversation.com (Mar. 12, 2014), https://theconversation.com/how-europes-data-privacy-reform-could-cost-australian-business-24210.
[47] Jan Philipp Albrecht, Member of the European Parliament and Rapporteur of the European Parliament's Civil Liberties, Justice and Home Affairs Committee (LIBE), Keynote at BCLT Privacy Law Forum Silicon Valley (Mar. 14, 2014); *see also* Laurits R. Christensen, Andrea Colciago, Federico Etro & Greg Rafert, THE IMPACT OF THE DATA PROTECTION REGULATION IN THE E.U. 11 (2013).
[48] Laurits R. Christensen, Andrea Colciago, Federico Etro & Greg Rafert, THE IMPACT OF THE DATA PROTECTION REGULATION IN THE E.U. 8 (2013).
[49] *Id*. at 4, 8.

appointed, consulting the responsible DPA in the case of risky personal data processing would no longer be required - the matter could be referred to the DPO.[50]

D. Data Breach Notifications

Another new obligation of the GDPR is the introduction of a comprehensive data breach notification requirement. That means that in the case of a personal data breach the controller will have to notify the responsible supervisory authority in the EU,[51] and additionally under certain circumstances, the affected data subjects without undue delay.

This requirement of a general data breach notification of the responsible DPA as well as the affected data subjects is new to many Member States. The revised EU Data Protection Directive 2009/136/EC of 2009[52] (revised ePrivacy Directive), which regulates data protection in the specific telecommunication and electronic communications sector and applies to all matters which are not specifically covered by the Data Protection Directive[53], currently requires in Article 4.3 telecommunication operators and Internet service providers to keep personal data confidential and secure, and to report to the competent national authority as well as to inform the concerned subscriber without undue delay when a personal data breach has occurred.[54] However, this notification requirement in the revised ePrivacy Directive only deals with breaches of personal data in the telecommunication and electronic communications sector.[55] A general data

[50] *Id*. at 11.
[51] *See infra* under Section II. 5. One-Stop-Shop Principle.
[52] Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No. 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws, 2009, O.J. (L 337/11) ("ePrivacy Directive").
[53] Andrej Savin, EU INTERNET LAW 211 (2013); Lukas Feiler, INFORMATION SECURITY LAW IN THE EU AND THE U.S. 112-116 (2012).
[54] Eur. Comm'n, *ePrivacy Directive – data breach notifications* (Jun. 24, 2013), http://ec.europa.eu/digital-agenda/en/eprivacy-directive-data-breach-notifications; *see also* Andrej Savin, EU INTERNET LAW 213 (2013); Lukas Feiler, INFORMATION SECURITY LAW IN THE EU AND THE U.S. 363-369 (2012).
[55] Lukas Feiler, INFORMATION SECURITY LAW IN THE EU AND THE U.S. 364 (2012).

breach notification requirement is currently neither provided in the Data Protection Directive nor in the revised ePrivacy Directive.[56]

In contrast to that, the provision of the proposed GDPR is much broader. According to Article 31.1 of the current version of the GDPR, "[i]n [the] case of a personal data breach, the controller shall without undue delay notify the personal data breach to the supervisory authority." And according to Article 32.1, "the controller shall, after the notification referred to in Article 31, communicate the personal data breach to the data subject without undue delay" when the personal data breach is likely to adversely affect the protection of the personal data, the privacy, the rights or the legitimate interests of the data subject. A data breach should be considered as adversely affecting the personal data or privacy of a data subject where it could result in, for example, identity theft or fraud, physical harm, significant humiliation or damage to reputation[57] of the subject. In addition, notifications to data subjects should be made not only as soon as reasonably feasible but also in close cooperation with the supervisory authority.[58]

The notification of the DPA must, according to Article 31.3, "at least: (a) describe the nature of the personal data breach including the categories and number of data subjects concerned and the categories and number of data records concerned; (b) communicate the identity and contact details of the data protection officer …; (c) recommend measures to mitigate the possible adverse effects of the personal data breach; (d) describe the consequences of the personal data breach; (e) describe the measures proposed or taken by the controller to address the personal data breach and mitigate its effects." The communication to the data subject, however, shall, pursuant to Article

[56] However, in single Member States such a general data breach notification requirement already exist, e.g. in Germany, Bundesdatenschutzgesetz [BDSG] [Federal Data Protection Act], Dec. 20, 1990, Bundesgesetzblatt [BGBl.] I S. 2954, as amended, § 42a (Ger.).
[57] General Data Protection Regulation – Consolidated Version of LIBE, Recital (67).
[58] *Id.*

32.2, "be comprehensive and use clear and plain language. It shall describe the nature of the personal data breach and … information about the rights of the data subject, including redress."

Therefore, not only EU companies but also companies from foreign countries like the U.S. will have to notify the responsible DPA as well as the affected data subjects without undue delay when a breach of personal data occurs, regardless of the type of personal data, the controller's business sector or the processor's business sector. According to the European Commission, it should be presumed that "without undue delay" means "not later than 72 hours".[59] If applicable, an explanation of the reasons for the delay should accompany the notification.[60]

Also this new legal requirement means that for U.S. IT companies which are dealing with the personal data of EU residents, there will be additional organizational, procedural and financial burdens.[61] In order to be compliant with the proposed GDPR companies have to specially set up reliable and sufficiently fast notification systems that are able to notify the responsible DPA as well as the affected data subjects immediately with the required information. This is extremely demanding, especially for non-serious data breaches, because these will also fall under the new regulation.[62]

However, this new requirement will generally not affect U.S. companies too severely because after the introduction of the Data Breach Notification Law in California in 2002,[63] security breach notification laws have been enacted in most U.S. states.[64] Because of that, most of the IT

[59] *Id.*
[60] *Id.*
[61] Laurits R. Christensen, Andrea Colciago, Federico Etro & Greg Rafert, THE IMPACT OF THE DATA PROTECTION REGULATION IN THE E.U. 4, 17 (2013).
[62] *Id.* at 4, 17, 42.
[63] Cal. Civ. Code §§ 1798.29, 1798.80 *et seq.* (2002).
[64] National Conference of State Legislatures (NCSL), State Security Breach Notification Laws (Jan. 21, 2014), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

companies in the U.S. that are amenable to the proposed new regulation will probably already have such notification systems and organizational procedures in place.

E. One-Stop-Shop Principle

Besides the planned harmonization of EU data protection law, there is from a legal as well as from a business perspective another advantage of the new data protection regime: the so-called one-stop-shop principle ("one company – one DPA").[65] According to this provision, U.S. companies will in the future only have to deal with one single national DPA that is in the EU country where the company has its main establishment.[66] In case where a company has more than one establishment in the EU one DPA will be the lead DPA.[67]

In comparison to this proposed regulation, today when a U.S. company is doing business in the EU it has to communicate with several national DPAs and, in case of Germany, even with several state DPAs, depending where it has establishments. This makes it currently quite complex and costly for companies, such as Google and eBay, which have not only one but several establishments in the EU.

However, Article 54a.1 of the proposed GDPR states explicitly: "Where the processing of personal data takes place in the context of the activities of an establishment of a controller or a processor in the Union, and the controller or processor is established in more than one Member State, or where personal data of the residents of several Member States are processed, the supervisory authority of the main establishment of the controller or processor shall act as the lead authority …." According to Article 4.13 of the proposed GDPR, "'main establishment' means the

[65] Press Release, Eur.Comm'n., Progress on EU data protection reform now irreversible following European Parliament vote (Mar. 12, 2014) (on file with author).
[66] Eur. Parl., *Q&A on EU data protection reform*, europarl.europa.eu, http://www.europarl.europa.eu/news/de/ news-room/content/20130502BKG07917/html/QA-on-EU-data-protection-reform (Mar. 4, 2014).
[67] *Id.*

place of establishment of the undertaking … in the Union, … where the main decisions as to the purposes, conditions and means of the processing of personal data are taken. …" Therefore, it does not matter where the processing of personal data is actually carried out.[68]

That means if U.S. IT companies have several establishments in the EU, in future only one single supervisory authority would act as the single contact point and the lead authority responsible for supervising the company throughout the EU to take all related decisions, e.g. in case of data breach notifications, the establishment of binding corporate rules, etc.[69] On the company side, the entity communicating with the lead authority will be the establishment where the company's main management decisions concerning data processing are taken. The rationale for this one-stop-shop approach is to have only one DPA – the DPA of the company's main establishment – which is competent for all of the company's data processing activities in the EU.

Contrary to the initial European Commission's position that adopted a true one-stop-shop approach, the current compromise text of the GDPR takes only an intermediate position and creates a "lead DPA system". That means, according to the recent version of the GDPR, that one lead DPA among the several DPAs will be the sole authority empowered to take legal decisions with regard to each company. However, this lead DPA will have complex cooperation obligations with regard to other DPAs responsible for their respective companies. Furthermore, individuals could lodge a complaint before the DPA of their home jurisdiction, and the lead DPA would be required to coordinate its work with that other DPAs. This could be quite complex – but primarily for the DPAs itself, and not for the companies.

[68] General Data Protection Regulation – Consolidated Version of LIBE, Recital (27).
[69] *Id*. Recital (97).

However, this new one-stop-shop system will make it generally simpler and cheaper for multinational U.S. companies that to do business in the EU because in the future they have to deal there only with one single national DPA.[70] Against this background this new provision will especially simplify for U.S. companies in the EU the establishment of each company's Binding Corporate Rules (BCR) and streamline their approval process, as the rules will be approved by a single DPA instead of several.

F. Sanction System

The downside is that within the new GDPR a strict sanction system with severe penalties is planned. That means that in case of non-compliance the responsible DPA may impose on U.S. companies fines of up to 100,000,000 EUR or up to 5% of the annual worldwide turnover.

Currently, the Data Protection Directive only imposes a rather broad and indefinite framework for sanctions in case of non-compliance and leaves the concrete implementation to the Member States.[71] Article 24 of the Data Protection Directive states generally that "… Member States shall adopt suitable measures to ensure the full implementation of the provisions of this Directive and shall in particular lay down the sanctions to be imposed in case of infringement of the provisions adopted pursuant to this Directive."[72]

In contrast, the provisions of the new GDPR are much stricter and much more specific in comparison to the Data Protection Directive. According to Article 79.2a. of the current version of the GDPR, "[for] anyone who does not comply with the obligations laid down in this Regulation, the supervisory authority shall impose at least one of the following sanctions: a) a warning in

[70] Press Release, Eur.Comm'n., Progress on EU data protection reform now irreversible following European Parliament vote (Mar. 12, 2014) (on file with author).
[71] Andrej Savin, EU INTERNET LAW 201 (2013).
[72] E.g. in Germany this framework provision of the EU Data Protection Directive 95/46/EC led to a sanction system with fines up to 300,000 EUR, Bundesdatenschutzgesetz [BDSG] [Federal Data Protection Act], Dec. 20, 1990, Bundesgesetzblatt [BGBl.] I S. 2954, as amended, § 43(3) (Ger.).

writing in cases of first and non-intentional non-compliance; b) regular periodic data protection audits; c) a fine up to 100,000,000 EUR or up to 5% of the annual worldwide turnover in case of an enterprise, whichever is greater."

Under this text, any violation of data processing requirements would subject the company to one of the three mentioned sanctions. That means that imposition of one of these sanctions is mandatory. However, the current version of the GDPR sets in Article 79.2c a list of mitigating factors such as the nature, gravity and duration of the non-compliance, the intentional or negligent character of the infringement, the repetitive nature of the infringement, the degree of co-operation with the supervisory authority, the specific categories of data affected, the level of damage, the action taken by the controller or processor to mitigate the damage, and any financial benefits intended or gained.[73] Interestingly, in the first draft of the GDPR, unveiled by the European Commission on 25 January 2012, only fines of up to EUR 1,000,000 or 2% of the annual worldwide turnover were proposed. This was one major points of the GDPR that were amended within the European Parliament's Civil Liberties, Justice and Home Affairs Committee (LIBE).

Against the background of this new harsh sanction system, which comes close to the sanctions imposed for anti-trust infringements, U.S. companies should take compliance with the new EU data protection regime seriously. That means that they have to build up their knowledge of EU data protection law, hire employees for the data protection and compliance department, and set up new policies, trainings, procedures and communication channels for this purpose.

[73] General Data Protection Regulation – Consolidated Version of LIBE, Recital (120); Eur. Parl., *Q&A on EU data protection reform*, http://www.europarl.europa.eu/news/de/news-room/content/2013502BK G07917/html/QA-on-EU-data-protection-reform (Mar. 4, 2014).

III. Selected Rights

A. Right to Erasure

As set out in the current version of the GDPR, one of the selected rights, which is of special interest for U.S. IT companies, is the right to erasure. This means that in the future personal data of EU residents will generally have to be deleted when the data is no longer needed, the data subject has withdrawn his or her consent, the storage period has ended, or the data has been processed illegally.

Such a subject's right to erasure is generally not new to European data protection law. The current Data Protection Directive already comprises different rules on the deletion of personal data.[74] Article 6.1(d) of the Data Protection Directive provides "that personal data must be: … (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete … are erased or rectified." Additionally, Article 12(b) and 12(c) of the Data Protection Directive provide that "Member States shall guarantee every data subject the right to obtain from the controller: … (b) as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data; (c) notification to third parties to whom the data have been disclosed of any rectification, erasure or blocking carried out in compliance with (b), unless this proves impossible or involves a disproportionate effort."

[74] Therefore, the Member States have generally already enacted such a right to erasure, e.g. in Germany, Bundesdatenschutzgesetz [BDSG] [Federal Data Protection Act], Dec. 20, 1990, Bundesgesetzblatt [BGBl.] I S. 2954, as amended, § 35(2) (Ger.); *see also* Andrej Savin, EU INTERNET LAW 198, 207 (2013); Alessandro Mantelaro, *The EU Proposal for a General Data Protection Regulation and the roots of the 'right to be forgotten'*, 29 CLSR 229, 232-233 (2013).

Therewith, both these rules limit an endless collection of personal data and set out different parameters under which personal data have to be erased.[75]

Although the general idea is quite analogous to the above mentioned provisions of the Data Protection Directive, the right to erasure set out in the current version of the GDPR is even more comprehensive. Article 17.1 of the proposed GDPR states:

> The data subject shall have the right to obtain from the controller the erasure of personal data … and to obtain from third parties the erasure of any links to, or copy or replication of that data, where one of the following grounds applies: (a) the data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; (b) the data subject withdraws consent on which the processing is based …, or when the storage period consented to has expired … (c) the data subject objects to the processing of personal data …; (d) the data has been unlawfully processed.

That means in the future data subjects will have the right to have their personal data erased under several circumstances – e.g. where the data is no longer necessary, where the individual withdraws his consent or objects to the processing of personal data, where the consented storage period has expired or where the data processing was unlawful. This also includes data passed on to third parties.[76] However, this new and comprehensive right to erasure will not be absolute because the current draft regulation includes in Article 17.3. several exceptions, e.g. for exercising the right of freedom of expression, for reasons of public interest in the area of public

[75] Alessandro Mantelaro, *The EU Proposal for a General Data Protection Regulation and the roots of the 'right to be forgotten'*, 29 CLSR 229, 233 (2013).
[76] General Data Protection Regulation – Consolidated Version of LIBE, Recital (54).

health, for historical, statistical and scientific research purposes and for compliance with a legal obligation to retain the personal data.[77]

This comprehensive, but non-absolute, right to erasure will force IT companies in the U.S. to adapt their organizational and technical processes in order to be compliant with the future EU data protection law. According to the proposed text of the GDPR, on the data subject's request the respective controller will have to erase links, copies and replications of personal data as well as inform third parties which are processing such data about data subject's request.

Interestingly, in the first draft of the GDPR, which was unveiled by the European Commission on 25 January 2012, the right to erasure was much stricter and comprised an even more comprehensive so called "right to be forgotten".[78] However, after numerous debates and lobbying, the rapporteur of European Parliament's Civil Liberties, Justice and Home Affairs Committee (LIBE), Jan-Philipp Albrecht, accepted the suggestion to change the right to be forgotten to the somewhat weaker right to erasure. Unlike the right to be forgotten, the right to erasure does not oblige companies to delete every information relating to a data subject from the Internet.

B. Right to Access and to Obtain Data for the Data Subject

The right to access and to obtain data for the data subject (so called "right of data portability") is one of the true innovations of the GDPR and is intended to regulate especially data processing in the field of social media. Under this new provision data subjects will be able to request a copy of

[77] *Id.* Recital (53); *see also* David Perera, *European Parliament votes for tighter data protection regulations* (Mar. 13, 2014), http://www.fiercegovernmentit.com/story/european-parliament-votes-tighter-data-protection-regulations/2014-03-13.

[78] Susanne Dehmel & Nils Hullen, *Auf dem Weg zu einem zukunftsfähigen Datenschutz in Europa? Konkrete Auswirkungen der DS-GVO auf Wirtschaft, Unternehmen und Verbraucher*, 3 ZD 147, 151 (2013).

personal data being processed in a format usable by this person and be able to transmit it electronically to another processing system.

This right of data portability is generally new to European data protection law. Although Article 12.(a) of the Data Protection Directive already "guarantee[s] every data subject the right to obtain from the controller: (a) …confirmation as to whether or not data relating to him are being processed and information at least as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed, communication to him in an intelligible form of the data undergoing processing and of any available information as to their source", current EU data protection law does not comprise an explicit right of data portability.

However, according to Article 15.2(a) of the current version of the GDPR:

> [T]he data subject [has] the right to obtain from the controller a copy of the provided personal data in an electronic and interoperable format which is commonly used and allows for further use by the data subject without hindrance from the controller from whom the personal data are withdrawn. Where technically feasible and available, the data shall be transferred directly from controller to controller at the request of the data subject.

That means when this version of the GDPR is in force, people will have the right to get their personal data from the company which holds it in a commonly used and interoperable electronic format. This new rule will make it easier for users to transfer their personal data (such as contact lists, previous emails, photos, etc.) between different service providers (e.g. from Facebook to

Google+ or from GMail to Yahoo).[79] Although this new subject's right of data portability cannot be seen as a key aspect of data protection (it is more a functional requirement for social networks and cloud providers) it will give consumers greater control over their personal data.

There are also ensuing technical consequences for IT companies. Similar to the right of erasure, this right of data portability will require companies, especially social network and cloud providers, to adapt their organizational and technical processes as well as their data formats accordingly. That means that firms will have to develop or implement data management systems that allow users to obtain personal data in structured and commonly used electronic formats.[80] However, according to the European Commission companies should be encouraged to develop and agree on interoperable industry standards by means of self-regulation.[81]

C. Data Protection by Design and by Default

This provision is also generally new to the European data protection legislation. Data protection by design and by default generally requires that data privacy standards be already designed into the development of new business processes for products and services, and that privacy settings are generally set at a high level by default.

Although the current Data Protection Directive states in Article 6.1(c) that "personal data must be … not excessive in relation to the purpose for which they are collected and/or further processed"

[79] Press Release, Eur.Comm'n., Progress on EU data protection reform now irreversible following European Parliament vote (Mar. 12, 2014) (on file with author); Eur. Parl., *Q&A on EU data protection reform* (Mar. 4, 2014), http://www.europarl.europa.eu/news/de/news-room/content/20130502BKG07917/html/QA-on-EU-data-protection-reform.

[80] Laurits R. Christensen, Andrea Colciago, Federico Etro & Greg Rafert, THE IMPACT OF THE DATA PROTECTION REGULATION IN THE E.U. 3 (2013).

[81] General Data Protection Regulation – Consolidated Version of LIBE, Recital (51a); Alexander Roßnagel, Philipp Richter, Maxi Nebel, *Besserer Internetdatenschutz für Europa – Vorschläge zur Spezifizierung der DS-GVO*, 3 ZD 103, 107 (2013).

the provision of data protection by design and by default is absolutely new in its extent and also one of the main technical and organizational changes that the GDPR will bring for IT companies.

The new requirements of data protection by design are provided for in Article 23.1 of the current version of the GDPR, which states:

> Having regard to the state of the art, current technical knowledge, international best practices and the risks represented by the data processing, the controller and the processor … shall … implement appropriate and proportionate technical and organisational measures and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject …. Data protection by design shall have particular regard to the entire lifecycle management of personal data from collection to processing to deletion, systematically focusing on comprehensive procedural safeguards regarding the accuracy, confidentiality, integrity, physical security and deletion of personal data.

Privacy by default is provided for in Article 23.2, which states:

> The controller shall ensure that, by default, only those personal data are processed which are necessary for each specific purpose of the processing and are especially not collected, or retained or disseminated beyond the minimum necessary for those purposes, both in terms of the amount of the data and the time of their storage. In particular, those mechanisms shall ensure that by default personal data are not made accessible to an indefinite number of individuals and that data subjects are able to control the distribution of their personal data.

That means that IT companies in the future should already at an early stage take the principles and obligations of data protection into account. More explicitly, these new principles of data protection by design and by default have the consequence that IT companies – and not only EU companies but also those from abroad – will have to be compliant with EU data protection provisions during the design phase. That means that a company should, at the product development stage, think, for example, about the amount of data it wants to collect in relation to the purpose, and the limitation that people may have access to personal data.

For many companies in the IT sector this new data protection requirement will mainly lead to huge changes in business procedures and practices, especially in the process of designing and developing new products. Data protection experts will have to be involved at an early stage in order to ensure strong data protection by design and strong data protection settings by default. In addition, the principle of data protection by design requires data protection to be embedded within the entire life cycle of the technology, from the very early design stage, right through to its ultimate deployment, use and final disposal.[82] The principle of data protection by default, however, requires privacy settings on services and products which should by default comply with the general principles of data protection, such as data minimization and purpose limitation.[83] From a practical perspective, compliance with this new requirement could be undertaken by the newly implemented DPO.[84] The DPO could be consulted prior to the design, procurement, development and setting-up of new systems and products in a company, in order to ensure compliance with the principles of privacy by design and privacy by default.[85]

[82] *Id*. Recital (54).
[83] *Id*. Recital (61).
[84] *Id*. Recital (75).
[85] *Id*. Recital (75).

IV. Conclusion

As described above, the proposed GDPR will not only bring advantages, but also additional data protection burdens to IT companies in the U.S.

On the one hand, the harmonization of data protection law across all 28 Member States will make business of multinational U.S. companies in the EU in the future much easier. Such companies only have to comply with a single set of data protection rules – and not with 28 different data protection laws – when they offer products or services to customers based in the EU. Additionally, the new one-stop-shop system will make it simpler and cheaper for multinational U.S. companies to do business in the EU because in the future such companies only have to deal with one responsible DPA[86], which will make it, for example, much easier to establish binding corporate rules in the EU.[87]

On the other hand, the current version of the GDPR also comprises various new and strengthened data subjects' rights, like the right to erasure, the right to access and obtain data for the data subject as well as the new principle of data protection by design and by default. According to the scope of the new regulation, the data subjects' rights will also apply directly to U.S. companies without any establishment in the EU, only if they process personal data of EU residents. In addition to that, the new EU data protection law also requires U.S. companies without any establishment in the EU, but handling personal data of EU residents, to appoint a DPO within the EU.

[86] Press Release, Eur.Comm'n., Progress on EU data protection reform now irreversible following European Parliament vote (Mar. 12, 2014) (on file with author), *see also* Laurits R. Christensen, Andrea Colciago, Federico Etro & Greg Rafert, THE IMPACT OF THE DATA PROTECTION REGULATION IN THE E.U. 4, 10, 42-43 (2013).
[87] Laurits R. Christensen, Andrea Colciago, Federico Etro & Greg Rafert, THE IMPACT OF THE DATA PROTECTION REGULATION IN THE E.U. 4 (2013).

Against this background, IT companies in the U.S. that do business within the EU or with its residents have to be attentive and should start preparing now for this fundamental and harsh change in the European data protection landscape. Companies should take these coming changes very seriously because regulators will be equipped with strong powers to enforce the new regulations.[88] For example, DPAs will be able to fine companies who do not comply with EU data protection rules up to 100,000,000 EUR or 5% of the annual worldwide turnover, whichever is greater.

From the practical side, compliance with the proposed GDPR will require significant investments and resources. Some of the new provisions will require the development of written policies and procedures, documentations, organizational structures and applications that are necessary to comply with the new rules. Security breaches will have to be disclosed, and incident response plans will have to be created accordingly. Companies' IT, legal and data privacy departments will need to more substantial budgets in order to hire or finance experienced staff, carry out training, and establish policies, procedures and technologies that will be needed to implement the new provisions.[89] In addition to that, provisions which limit the use of personal data (such as data protection by design and by default) will also impact on the business itself.[90] For example, due to the required high data protection settings by default, marketing measures are in the future may not be as targeted and successful as before. Against this background, it can be assumed that the overall costs and losses of data protection compliance will significantly increase, in particular for Small and Medium-Sized Enterprises (SME).[91] That means that complying with the complex new

[88] Press Release, Eur.Comm'n., Progress on EU data protection reform now irreversible following European Parliament vote (Mar. 12, 2014) (on file with author).
[89] Laurits R. Christensen, Andrea Colciago, Federico Etro & Greg Rafert, THE IMPACT OF THE DATA PROTECTION REGULATION IN THE E.U. 1 (2013).
[90] *Id*. at 1, 9.
[91] *Id*. at 1, 42.

EU data protection law is likely to have a substantial negative impact on business, innovation and employment, and it is likely to be prohibitively expensive for non-EU SMEs interacting on the European market.[92] However, companies with already strong procedures for protecting personal data and large companies will have a competitive advantage on a global scale, and will be able to afford to enter or remain in the European market under the new GDPR.[93]

Although still many steps have to be taken before the new regulation will become law, the current version of the GDPR already provides a binding starting point for the negotiations between the EU Parliament and the European Council of Ministers. The final text will very likely differ from the current version, but in any case, the future regulation will significantly impact on how companies collect, use and share personal data both within the EU and globally.[94]

While that means that the adoption of the final GDPR may still be some time away, the clock for U.S. IT companies to prepare for the great change is already ticking!

* * * * *

[92] Dan Jerker B. Svantesson, *How Europe's data privacy reform could cost Australian business* (Mar. 12, 2014), https://theconversation.com/how-europes-data-privacy-reform-could-cost-australian-business-24210; *see also* Laurits R. Christensen, Andrea Colciago, Federico Etro & Greg Rafert, THE IMPACT OF THE DATA PROTECTION REGULATION IN THE E.U. 1, 4, 6-7, 10, 27, 29, 43 (2013); Susanne Dehmel & Nils Hullen, *Auf dem Weg zu einem zukunftsfähigen Datenschutz in Europa? Konkrete Auswirkungen der DS-GVO auf Wirtschaft, Unternehmen und Verbraucher*, 3 ZD 147, 152 (2013).

[93] Dan Jerker B. Svantesson, *How Europe's data privacy reform could cost Australian business*, theconversation.com (Mar. 12, 2014), https://theconversation.com/how-europes-data-privacy-reform-could-cost-australian-business-24210.

[94] *See also* 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, 55, 61 (2014).