Internal Compliance Mechanisms for Firms in the EU General Data Protection Regulation

W. Gregory Voss

Internal Compliance Mechanisms for Firms in the EU General Data Protection Regulation

*W. Gregory Voss**

Le Règlement général de l'UE sur la protection des données : quelles implications pour l'organisation interne des entreprises?

El Reglamento General de Protección de Datos de la UE : implicaciones para la organización interna de las empresas

O Regulamento Geral sobre a Proteção de Dados da UE : Algumas Implicações para a Organização Interna das Empresas

《欧盟一般数据保护条例》中的公司内部合规机制

Résumé

Le nouveau règlement général sur la protection des données dans l'UE (RGPD) fait naître des obligations et comprend des incitatifs liés à l'élaboration de mécanismes internes de conformité qui n'existent pas dans la législation actuelle. Ces obligations, telles que celles, dans certains cas, de désigner un délégué à la protection des données, de mener une analyse d'impact relative à la protection des données ou d'effectuer une notification d'une violation des données à caractère personnel, auront un impact sur les processus

Abstract

The new EU General Data Protection Regulation (GDPR) establishes requirements (and certain incentives) for internal compliance mechanisms that do not exist in current legislation. These requirements, which will have an impact on internal processes and staffing of firms, such as the requirement in certain cases of engaging a data protection officer, of conducting a data protection impact assessment, or making notifications of data breaches, will require firms to organize themselves prior to the GDPR becoming

* University of Toulouse/Université de Toulouse, Toulouse Business School.

internes ainsi que sur l'organisation du personnel des entreprises. Ainsi, elles obligeront ces dernières à revoir leurs manières de faire d'ici la date de la mise en application du RGPD en 2018. Cet article expose d'abord le champ d'application territorial accru du RGPD, avant de discuter de la responsabilisation augmentée des entreprises et plus précisément des analyses d'impact relatives à la protection des données, de la consultation et de l'autorisation préalables, des délégués à la protection des données et des notifications d'une violation des données à caractère personnel. Ce faisant, certaines divergences entre les différentes versions préliminaires du RGPD sur ces points seront évoquées. Enfin, certains éléments qui inciteront les entreprises à se mettre en conformité avec le RGPD seront soulignés.

Resumen

El nuevo Reglamento General de Protección de Datos de la UE (RGPD) crea obligaciones e incluye incentivos relacionados con la elaboración de mecanismos internos de cumplimiento que no existen en la legislación vigente. Estas obligaciones, como las de designar a un encargado de protección de datos, realizar una evaluación de impacto relacionada con la protección de datos o notificar una violación de datos personales, en algunos casos, tendrán un impacto en los procesos internos, así como en el manejo del personal de las empresas. De ese modo, van a obligar a estas últimas a revisar sus prácticas antes de la fecha de aplicación del RGPD en 2018. Este artículo expone inicialmente la ampliación del campo de aplicación territorial del RGPD, antes de

applicable in 2018. This article sets out first the increased territorial scope of the GDPR, prior to discussing the increased accountability of firms, focusing on data protection impact assessments, prior consultation and prior authorization, data protection officers, and data breach notifications. On the way, certain differences among the various versions of the GDPR prior to its adoption on these points will be discussed. Finally, incentives for compliance are highlighted.

Resumo

O novo Regulamento Geral sobre a Proteção de Dados (RGPD) da UE estabelece obrigações e compreende incentivos ligados à elaboração de mecanismos internos de conformidade que não existem na legislação atual. Essas obrigações, tais como, em certos casos, as de designar um responsável pela proteção de dados, de realizar uma análise de impacto relativo à proteção dos dados ou de efetuar uma notificação de uma violação de dados de caráter pessoal, terão um impacto sobre os processos internos como também sobre a organização do pessoal das empresas. Assim, obrigarão estas últimas a se organizarem até a data de entrada em vigor do RGPD em 2018. Este artigo expõe primeiramente o campo de aplicação territorial ampliado do RGPD, antes de

discutir sobre el incremento de la responsabilidad de las empresas, y más específicamente, sobre las evaluaciones de impacto relativas a la protección de datos, la consulta y autorización previas, los encargados de protección de datos y las notificaciones de violación de datos personales. En este contexto, se mencionarán algunas divergencias entre las diferentes versiones preliminares del RGPD sobre estos puntos. Para concluir, se resaltarán ciertos elementos que alentarán a las empresas a cumplir con el RGPD.

discutir a responsabilização aumentada das empresas e mais precisamente das análises de impacto relativas à proteção de dados, da consulta e da autorização prévias, dos responsáveis pela proteção de dados e das notificações de uma violação de dados de caráter pessoal. Durante a exposição, serão evocadas certas divergências entre as diferentes versões preliminares do RGPD sobre esses pontos. Por fim serão sublinhados certos elementos que incentivarão as empresas a se colocarem em conformidade com o RGPD.

摘要

新的《欧盟一般数据保护条例》对当前立法中没有的内部合规机制做出了规定（以及部分激励机制）。这些规定，比如某些情况中，规定数据保护官开展数据保护影响评估，或者做出数据违规通知，将影响到公司的内部程序及人事管理，并且要求公司在该条例于2018年生效之前做好调整。本文首先阐述了该条例不断扩大的地域适用范围，然后探讨了不断增加的公司责任，尤其关注数据保护影响评估、事先征询与事先批准机制、数据保护官以及数据违规通知。其中，还会讨论该条例通过之前各种版本关于这个些问题的差异。最后，着重考查了合规激励机制。

Plan de l'article

The concern for the protection of "personal data" or "personal information" has grown with the rapid expansion of data processing capacities and the explosion of the medium known as the internet. Different jurisdictions have handled the concern in various ways. Two authors have chosen to classify these ways in three models: comprehensive (or omnibus), such as the laws of the European Union; co-regulatory, such as Canada's *Personal Information, Protection and Electronic Documents Act* of 1998 (PIPEDA); and a self-regulatory/sectorial approach found in the United States.[1] Another author refers to the United States model as a "consumer protection model" that "emerged out of a vacuum" as opposed to the "data protection" model of the European Union where "legal rules about data handling were specifically designed from the outset to protect individual privacy or data security."[2] The Organization for Economic Co-operation and Development (OECD)'s Guidelines set out basic principles of national application (collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation, and accountability).[3] These Guidelines may be seen as "a consensus position of countries from North America, Europe, and East Asia as to the basic structure of privacy law."[4] However, of the two extremes to the specific range of three models set out above – those of the European Union and the United States – the former is seen to have had a considerable impact internationally, while the latter has evidenced a "relative lack of American influence on worldwide information privacy regulatory models."[5] This study will

---

1 John Black and Mike Dunne, « Chapter 8: Information Security », in Juliet M. Moringiello (ed.), *Internet Law for the Business Lawyer*, 2nd ed., Chicago, American Bar Association, 2012, p. 169.

2 William McGeveran, *Privacy and Data Protection Law*, University Casebook Series, Thomson Reuters, 2016.

3 OECD, *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, 23 septembre 1980, Doc. Off. OECD C(80)58/FINAL.

4 Daniel J. Solove and Paul M. Schwartz, *Information Privacy Law*, 5th ed., New York, CCH Incorporated, Wolters Kluwer, 2015, p. 1098.

5 Paul M. Schwartz, « The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures », (2013) 126 *Harvard Law Review* 1966, 1966-1967. See also: D. J. Solove and P. M. Schwartz, *id.*, p. 1096: "Outside of Europe, other countries from around the world are moving toward adopting comprehensive privacy legislation on the European model." For the view of one author of the "ratcheting up" effect of EU law on U.S. privacy law, see: Gregory Shaffer, « Globalization and Social Protection: the Impact of EU and International Rules in the Ratcheting up of US Privacy Standards », (2000) 25 *Yale Journal of International Law* 1, 7.

focus on the former – the approach of the European Union – while keeping in mind the other systems.

The development of European Union data protection legislation has now entered its third phase, more than forty-five years after the first legislation adopted by the German Federal *Land* of Hesse in 1970.[6] The first phase was the national phase when European nations (or sub-divisions, such as Hesse) adopted initial legislation. For example, Germany adopted the *German Federal Data Protection Act* of 1977 (BDSG) in 1977.[7] Earlier, in 1973 Sweden adopted its data protection legislation and other nations followed: "Austria (1978), Denmark (1978), France (1978), and Norway (1978) (citations omitted)."[8] By the end of this phase, "there was a consensus that information privacy statutes were to be constructed around Fair Information Practices (FIPs)," whether this be in the United States or in Western Europe.[9] Notably, in the middle of this first phase an international instrument was adopted as well: the Council of Europe's Convention 108 – the first binding international treaty in the area of data protection – which has been adopted by the European Union, in addition to other European and non-European nations, and contains requirements for contracting parties to protect individual rights and freedoms in connection with the automatic processing of their personal data[10].

The second phase in the development of European data protection legislation, which has recently drawn to a close, is one of relative harmonization through the national implementation of a common European legislative instrument. Currently the national data protection legislation of the twenty-eight European Union (EU) Member States implements the 1995 Data Protection Directive (DP Directive)[11]. When new legislation was pro-

6 P. M. Schwartz, *supra*, note 5, p. 1969.

7 For a discussion of this legislation, see: J. Lee Riccardi, « The German Federal Data Protection Act of 1977: Protecting the Right to Privacy? », (1983) 6 *B.C. Int'l & Comp. L. Rev.* 243.

8 P. M. Schwartz, *supra*, note 5, p. 1969.

9 *Id.*

10 Council of Europe, *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, ETS No. 108, as amended, (January 28, 1981).

11 European Union, *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 « DP Directive »). For one example of a Member State act implementing the DP Directive, see: *Loi 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés*, J.O.

posed in 2012, the DP Directive was seen to have been inadequate in terms of harmonization. Indeed, a report was commissioned by the European Commission for the purpose of determining whether "differences (or divergences) in the way in which these laws are applied" and whether such differences or divergences constituted obstacles to the development of the internal market. In 2002, the resulting study was published.[12] Viviane Reding, who as Justice Vice Commissioner had been in charge of the data protection reform, highlighted the lack of harmonization under the DP Directive and the need for a new legal instrument:

> Although the objective of Directive 95/46/EC was to ensure an equivalent level of data protection within the EU, there is still considerable divergence in the data protection rules across member states. As a consequence, data controllers may have to deal with 27 different national data protection laws and requirements within the EU. The result is a fragmented legal environment which has created legal uncertainty and unequal protection for data subjects. This has caused unnecessary costs and administrative burdens for controllers, in particular for businesses operating across borders. This irregular protection constitutes a disincentive for enterprises and affects the competitiveness of European companies. At the same time, the fundamental right to the protection of personal data requires the same level of data protection for individuals throughout the Union. Additional common EU rules are therefore necessary to avoid the risk of different level of protection in the member states.[13]

However, that was not the only reason for data protection law reform: the DP Directive was also seen as outdated or obsolete in the sense that it had been adopted at a time when many current technologies had not yet been invented (e.g., biometrics, big data, cloud computing, etc.), and so had not been anticipated by the European legislators.[14]

---

7 janvier 1978, p. 227 (*Law 78-17 of Jan. 61978 on Information Technology, Data Files, and Civil Liberties*, J.O., Jan. 7, 1978, p. 227 (English translation)) (hereinafter « *French Data Protection Act* »).

12 Douwe Korff, *EC Study on Implementation of Data Processing Directive: Comparative Summary of National Laws*, September 2002, online: <http://194.242.234.211/documents/10160/10704/Stato+di+attuazione+della+Direttiva+95-46-CE> (consulted on September 15, 2017).

13 Viviane Reding, « The European data protection framework for the twenty-first century », (2012) 2(3) *International Data Privacy Law* 119, 121-129. Note that at the time Reding published her article Croatia had not yet joined the European Union, so there were then twenty-seven Member States.

14 In this sense, see: Mira Burri and Rahel Schär, « The Reform of the EU Data Protection Framework: Outlining Key Changes and Assessing Their Fitness for a Data-driven

The third phase – one of unification of European Union data protection law – has begun with the adoption of the EU General Data Protection Regulation (GDPR) proposed by Reding[15], which as a regulation will be applicable in the same form throughout the European Union, with effect from May 25, 2018, when it will repeal and replace the DP Directive.[16]

That date, when the GDPR is to be applicable, is two years from its date of entry into force, which occurred on May 24, 2016. The United Kingdom has voted to leave the European Union and the official procedure for what has been called "Brexit" has begun, which if carried out to conclusion, would decrease the number of Member States in the European Union to twenty-seven. Nonetheless, in response to a question in Parliament on October 24, 2016, a member of the United Kingdom Government (Rt Hon Karen Bradley MP, Secretary of State for Culture, Media and Sport) expressed the view that the United Kingdom will "opt in" to the GDPR:

> We will be members of the EU in 2018 and therefore it would be expected and quite normal for us to opt into the GDPR and then look later at how best we might be able to help British business with data protection while maintaining high levels of protection for members of the public.[17]

Economy », (2016) 6 *Journal of Information Policy* 2; see also: Nathalie Martial-Braz, « Introduction » in Nathalie Martial-Braz (ed.), *La proposition de règlement européen relatif aux données à caractère personnel: propositions du réseau Trans Europe Experts*, Paris, Société de législation comparée, 2014, p. 13-14.

15 European Union, *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation)*, 2016 O.J. (L 119) 1 (hereinafter « GDPR »).

16 *Id.*, art. 94(1), p. 86.

17 United Kingdom, House of Commons, Culture, Media and Sport Committee, *Oral evidence: Responsibilities of the Secretary of State for Culture, Media and Sport, HC 764*, October 24, 2016, online: <http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/culture-media-and-sport-committee/responsibilities-of-the-secretary-of-state-for-culture-media-and-sport/oral/42119.html> (consulted on September 15, 2017). For a discussion of this statement by the head of the UK data protection agency (the Information Commissioner's Office, or ICO) see: Elizabeth Denham, *How the ICO will be supporting the implementation of the GDPR*, October 31, 2016, online: <https://iconewsblog.wordpress.com/2016/10/31/how-the-ico-will-be-supporting-the-implementation-of-the-gdpr/> (consulted on September 15, 2017).

The GDPR represents a major change in European Union legislation in the field of data protection. Not only is it formulated as a regulation, but also it takes a different focus than the DP Directive, based on accountability and compliance. European Data Protection Supervisor (EDPS) Giovanni Buttarelli has described the GDPR accountability requirements as meaning "being able to demonstrate compliance with the data protection rules – a shift from a merely bureaucratic compliance exercise."[18]

A proposal for the GDPR was initially communicated by the European Commission (Commission) in a draft presented on January 25, 2012 (Commission Draft)[19]. Two years later – on March 12, 2014 – the European Parliament (Parliament) voted in favor of an amended version of the GDPR in first reading in plenary session (Parliament Draft)[20]. The Council of Ministers of the European Union finally adopted a common negotiating position on the GDPR on June 15, 2015[21], by adopting the Justice and Home Affairs draft GDPR version of June 11, 2015 (Council Draft)[22],

18 Giovanni Buttarelli, *Privacy in an age of hyperconnectivity, Keynote speech to the Privacy and Security Conference 2016*, Rust am Neusiedler See, November 7, 2016, online: <https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2016/16-11-07_Speech_GB_Austria_EN.pdf> (consulted on September 15, 2017).

19 European Union, *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, January 25, 2012, online: <http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf> (consulted on September 15, 2017) (hereinafter « Commission Draft »).

20 European Union, *European Parliament legislative resolution of 12 March 2014 on 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)* (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)) (Ordinary legislative procedure: first reading), online: <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2f%2fEP%2f%2fTEXT%2bTA%2bP7-TA-2014-0212%2b0%2bDOC%2bXML%2bV0%2f%2fEN&language=EN> (consulted on September 15, 2017) (hereinafter « Parliament Draft »).

21 Council of Europe, Press Release, *Data Protection: Council agrees on a general approach*, June 15, 2015, online: <http://www.consilium.europa.eu/en/press/press-releases/2015/06/15-jha-data-protection/> (consulted on Septembre 15, 2017).

22 European Union, *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)* – Preparation of a general approach, June 11, 2015, online: <http://data.consilium.europa.eu/doc/

allowing a trilogue between the Council of the European Union (Council), the Commission and the Parliament to begin on June 24, 2015[23]. (The Commission Draft, the Parliament Draft, and the Council Draft shall be referred to herein collectively as the GDPR Drafts, each individually a GDPR Draft.) The trilogue finally led to a political agreement on the text of the GDPR on December 15, 2015[24], and this was cast into a final GDPR text adopted by the Council in first reading on April 8, 2016[25], which was then approved by the Parliament in second reading on April 14, 2016[26], and formally adopted on April 27, 2016. From time to time we will refer to the various GDPR Drafts for historical purposes.

Both the DP Directive and the GDPR provide broad definitions of the "personal data" that they protect, in contrast to North American legislation, although the latter may be seen as having "multiple competing definitions" for personal information, where "gaps and inconsistencies" are legion when compared to European legislation.[27] The European instruments do not require that the information covered by the definition actually identify the subject – it merely has to be information related to "an identified or identifiable natural person." It is enough that the individual may be

document/ST-9565-2015-INIT/en/pdf> (consulted on Septembre 15, 2017) (hereinafter « Council Draft »).

23 European Parliament, Press Release, *Data Protection: Parliament's Negotiators Welcome Council Negotiating Brief,* June 15, 2015, online: <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+IM-PRESS+20150615IPR66464+0+DOC+PDF+V0//EN&language=EN> (consulted on September 15, 2017).

24 European Union, Commission Regulation 5853/12, *Protection of individuals with regard to the processing of personal data, and the free movement of such data (General Data Protection Regulation)*, 2012 O.J. (L XXX), online: <http://www.emeeting.europarl.europa.eu/committees/agenda/201512/LIBE/LIBE%282015%291217_1/sitt-1739884> (consulted on September 15, 2017), p. 102.

25 Council of Europe, Press Release, *Data protection reform: Council adopts position at first reading*, April 8, 2016, online: <http://www.consilium.europa.eu/en/press/press-releases/2016/04/08-data-protection-reform-first-reading/> (consulted on September 15, 2017).

26 European Parliament, Press Release, *Data protection reform – Parliament approves new rules fit for the digital era,* April 14, 2016, online: <http://www.europarl.europa.eu/pdfs/news/expert/infopress/20160407IPR21776/20160407IPR21776_en.pdf> (consulted on September 15, 2017).

27 Paul M. Schwartz and Daniel J. Solove, « Reconciling Personal Information in the United States and European Union », (2014) 102 *Calif. L. Rev.* 877, 887.

indirectly identified by referring to certain information. The DP Directive provides that:

> 'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;[28]

The GDPR provides similarly that:

> 'Personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.[29]

This will of the European legislators to be very inclusive, even where no financial prejudice exists, has been noted by authors in North America.[30] It is also notable that the "genetic" nature of a person has been added in the GDPR, to take into account newer DNA-analysis technologies. In addition, "location data," linked to the developing use of GPS technology, and "online identifier[s]," have been added, which "modernize and expand the sweep" of the DP Directive.[31]

As an illustration of the reach of the definition of "personal data," a recent ruling of the Court of Justice of the European Union held that under the DP Directive a dynamic internet protocol (IP) address could be considered personal data where the party holding the IP address had the legal

---

28 DP Directive, *supra*, note 11, art. 2(a), p. 38.

29 GDPR, *supra*, note 15, art. 4(2), p. 33.

30 Vincent Gautrais, « L'approche Nord-Américaine : proposition de règlement général sur la protection des données: un regard d'ailleurs... », in Nathalie Martial-Braz (ed.), *La proposition de règlement européen relatif aux données à caractère personnel: propositions du réseau Trans Europe Experts*, Paris, Société de législation comparée, 2014, p. 464, at 479-480. For a thorough discussion of the concept of personal data (or personal information) from both sides of the Atlantic, see generally: P. M. Schwartz and D. J. Solove, préc., note 27.

31 P. M. Schwartz and D. J. Solove, *id.*, 886.

means to be able to identify the data subject with the help of the internet service provider and the competent authority:

> a dynamic IP address registered by an online media services provider when a person accesses a website that the provider makes accessible to the public constitutes personal data within the meaning of that provision, in relation to that provider, where the latter has the legal means which enable it to identify the data subject with additional data which the internet service provider has about that person.[32]

This position coincides with that adopted years earlier by the advisory Article 29 Data Protection Working Party, commenting that even dynamic IP addresses are data related to an identifiable natural person, with the help of an internet access provider, for example.[33] Moreover, given the similarity in the definitions of "personal data" in the DP Directive and the GDPR, a decision on the same fact pattern under the GDPR should provide the same result.

The GDPR, which is to become effective in 2018, contains various measures intended to secure compliance with its provisions. Some of them concern the internal organization of firms and will be the subject of our study. Their aim is to insure an increased accountability of firms (Section II), and to provide incentives for compliance (Section III). These developments will require firms to organize themselves prior to the GDPR becoming applicable in 2018.

However, before we commence our study on the impact of the GDPR on the internal compliance mechanisms of firms, we will first investigate the increased territorial scope of the proposed legislation on companies coming from outside the European Union (Section I), which makes our investigation of the various requirements of the GDPR all the more relevant.

---

[32] *Patrick Breyer* v. *Bundesrepublik Deutschland*, Case C-582/14, (October 12, 2016), online: <http://curia.europa.eu/juris/celex.jsf?celex=62014CJ0582&lang1=en&type=TXT> (consulted on September 15, 2017), par. 48-49.

[33] European Union, Article 29 Data Protection Working Party, *Working Document Privacy on the Internet – An Integrated EU Approach to On-line Data Protection* (WP 37), November 21, 2000, online: <ec.europa.eu/justice/policies/privacy/docs/wpdocs/2000/wp37en.pdf> (consulted on Septembre 15, 2017), p. 21.

I. Increased Territorial Scope of the GDPR

In order to understand the increased territorial scope of the GDPR (Section I B), and its implications for companies headquartered outside of the European Union, we will first look at the territorial scope of current European Union data protection law (Section I A).

A. Territorial Scope of the DP Directive

Under the current DP Directive, the relevant European Union Member State's data protection law applies when the data processing:

> is carried out in the context of the activities of an establishment of the controller on the territory of the Member State; when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable;[34]

Under the DP Directive, a "controller" is:

> the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data;[35]

In addition, where the controller is not established on European Union territory, data protection law of a European Union Member State would apply either (i) where it applies through the application of international public law ("the controller is not established on the Member State's territory, but in a place where its national law applies by virtue of international public law;"[36]); or (ii) where equipment located on the territory of a Member State is used for processing personal data, unless only for purposes of transit through the territory ("the controller is not established on Community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, 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."[37]). Two commentators

[34] DP Directive, *supra*, note 11, art. 4(1)(a), p. 39.
[35] *Id.*, art. 2(d), p. 38.
[36] *Id.*, art. 4(1)(b), p. 39.
[37] *Id.*, art. 4(1)(c), p. 39.

have suggested that this territorial scope, as transposed into French domestic law, has resulted in law-shopping. To illustrate this point, they cite a French case involving Google Groupes, where Google successfully argued that it had neither any establishment in France, nor any means, and that data was using equipment only for the purposes of transit through France.[38]

B. Territorial Scope of the GDPR

The GDPR applies to processing in the context of activities of an establishment of a controller in the European Union. It adds to the scope, however, processing in the context of activities of a processor ("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"[39]). A processor is "a natural or legal person, public authority, agency or other body, which processes personal data on behalf of the controller"[40].

Perhaps the most significant change regarding territorial scope in the GDPR, however, is that contained in the next paragraph. In the GDPR, that instrument will apply to a controller or processor who is not established in the EU and processes the personal data of subjects who are themselves in the EU, where the processing relates to the offering of goods or services to them (whether or not payment is required), or where their behavior within the EU is monitored:

> 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 behaviour as far as their behaviour takes place within the Union.[41]

---

38 Laure Marino and Romain Perray, « Les nouveaux défis du droit des personnes: la marchandisation des données personnelles », in Judith Rochfeld (ed.), *Les nouveaux défis du commerce électronique*, Paris, LGDJ, Lextenso éditions, 2010, p. 55, at 58-61.

39 GDPR, préc., note 15, art. 3(1), p. 32.

40 *Id.*, art. 4(8), p. 33.

41 *Id.*, art. 3(2), p. 33.

This language extends the provision to processing by *processors* as well as controllers. The language making lack of payment for goods or services non-dispositive reflects a change introduced in both the Parliament Draft and the Council Draft.

The activities covered by this article are thus twofold: first, where the processing activities are related to the offering of goods or services to a data subject in the EU, or the monitoring of the behavior of data subjects, where the behavior occurs in the EU (this limitation was introduced in the Council Draft and taken up again by the GDPR), such as through behavioral marketing, for instance. In these cases, the controller or processor, as the case may be, is required to designate a representative in the European Union ("Where Article 3(2) applies, the controller or the processor shall designate in writing a representative in the Union."[42]), unless:

(a) processing which is occasional, does not include, on a large scale, processing of special categories of data as referred to in Article 9(1) or processing of personal data relating to criminal convictions and offences referred to in Article 10, and is unlikely to result in a risk to the rights and freedoms of natural persons, taking into account the nature, context, scope and purposes of the processing; or

(b) a public authority or body.[43]

As made clear in the GDPR, this representative is meant to receive communications addressed to the controller by the EU data protection supervisory authorities and by data subjects:

> The representative shall be mandated by the controller or processor to be addressed in addition to or instead of the controller or the processor by, in particular, supervisory authorities and data subjects, on all issues related to processing, for the purposes of ensuring compliance with this Regulation.[44]

Nevertheless, legal actions may be brought against the controller or processor itself:

> The designation of a representative by the controller or processor shall be without prejudice to legal actions which could be initiated against the controller or the processor themselves.[45]

42 *Id.*, art. 27(1), p. 48.
43 *Id.*, art. 27(2), p. 48.
44 *Id.*, art. 27(4), p. 49.
45 *Id.*, art. 27(5), p. 49.

In addition, similarly to Member State law under the DP Directive, the GDPR applies when the processing occurs by a controller where Member State law applies by virtue of public international law:

> This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.[46]

Thus, companies headquartered outside of the EU, without an establishment there, may be subject to the GDPR, so long as they are processing personal data of a data subject in the EU in connection with the offering of goods or services to him or her, or monitoring his or her behavior, insofar as such behavior occurs in the EU, and they may have to appoint a representative in the EU.

These territorial provisions limit opportunity for law-shopping and may be seen to allow a more level playing field for European companies in the face of North American or even East Asian competitors in the borderless world of the internet. The German Telecommunications giant Deutsche Telekom AG's CEO Timotheus Höttges was quoted in their "Data Privacy and Data Security Report 2014," as then arguing for a swift adoption of the proposed General Data Protection Regulation, in part, one may infer, because of its extraterritorial application to non-European companies offering goods or services to European residents, or monitoring their behavior:

> It is high time that Europe and the US reached a mutual understanding of what data protection entails. The high standards of privacy in Europe are a blessing, but they are distorting competition in the digital economy. American businesses do almost whatever they want – but we permit ourselves very little. With this in mind, the proposed EU General Data Protection Regulation cannot enter into force soon enough. This would mean that all businesses serving EU citizens would have to work within the same parameters – including companies headquartered outside of Europe.[47]

---

46 *Id.*, art. 3(3), p. 33.

47 Deutsche Telekom AG, *Data Privacy and Data Security Report 2014*, February 23, 2015, online: <https://www.telekom.com/en/corporate-responsibility/data-protection---data-security/news/new-report--data-protection-and-data-security-362402> (consulted on September 15, 2017).

Now that we understand the increased territorial scope of the GDPR, by comparison with the DP Directive, we are ready to begin our discussion of the impact of the GDPR on the internal organization of firms.

II. Internal Compliance Mechanisms and Increased Accountability of Firms

Today, companies subject to EU data protection law must notify relevant Member State data protection agencies of automatic or semi-automatic processing of personal data, subject to certain exceptions[48]. Although this notification requirement would be eliminated in the GDPR, and the fact of having a more unified body of data protection law in Europe would yield benefits to companies of up to €2.3 billion per year according to the European Commission (savings due to the elimination of the notification requirement alone are estimated at €130 million)[49], in return firms would become more accountable, and would be required to implement compliance mechanisms that will be discussed below.

This concept of accountability, already present (without being explicitly identified as such) in the DP Directive, is further developed in the GDPR. As the Commission noted when the Commission Draft was proposed:

> Article 22 [Article 24 in the final GDPR] takes account of the debate on a "principle of accountability" and describes in detail the obligation of responsibility of the controller to comply with this Regulation and to demonstrate this compliance, including by way of adoption of internal policies and mechanisms for ensuring such compliance.[50]

---

48 DP Directive, *supra*, note 10, art. 18(1), p. 43-44. This notification requirement, together with its exemptions, is discussed in greater detail in W. Gregory Voss and Katherine Woodcock, *Navigating EU Privacy and Data Protection Law*s, Chicago, American Bar Association, 2015, p. 45-50.

49 European Commission, *EU Data Protection Reform: What benefits for businesses in Europe?,* January 2016, online: <http://ec.europa.eu/justice/data-protection/document/factsheets_2016/data-protection-factsheet_01a_en.pdf> (consulted on September 15, 2017).

50 Commission Draft, *supra*, note 18, p. 10. The Commission then foresaw that, as a result of the adoption of the Commission Draft, data subjects "will [...] encounter reinforced accountability of those processing personal data." *Id.*, at 103.

Already, 46% of privacy professionals who believe that their firms will be subject to the GDPR, report that one of the steps being taken to prepare for the GDPR is creating a new accountability framework, and 21% say that creating a new reporting structure is a step being taken by their organization.[51]

Some might see in this development of the principle of accountability the imprint of an American influence.[52] One commentator remarked that this Article on controller responsibility "slightly resembles the concept of accountability found in the Asia-Pacific Economic Cooperation (APEC) Privacy Framework"[53], which had an American influence, as well.

Whatever its origins, this accountability can be seen in the requirement that firms maintain certain records regarding processing activities[54], allowing the constitution of proof of compliance, and would necessitate the conducting of data protection impact statements in certain circumstances (Section II A), involve requirements for prior consultation before processing (and even prior authorization under the Commission Draft), in certain cases (Section II B), and for certain companies to have data protection officers (Section II C). In addition, personal data breach notifications are introduced as a requirement (Section II D). The end result would involve the creation of internal mechanisms for firms in order to allow them to comply with these new accountability requirements.

---

51 IAPP, *IAPP-EY Annual Privacy Governance Report 2016*, online: <https://iapp.org/media/pdf/resource_center/IAPP-2016-GOVERNANCE-SURVEY-FINAL2.pdf> (consulted on September 15, 2017), p. 97.

52 Winston Maxwell and Sarah Taïeb, « L'accountability, symbole d'une influence américaine sur le règlement européen des données personnelles? », (2016) 3 *Dalloz IP/IT* 123.

53 Francoise Gilbert, « Proposed EU Data Protection Regulation: The Good, the Bad, and the Unknown », (2012) 15(10) *Journal of Internet Law* 1, 26.

54 GDPR, *supra*, note 15, art. 30, p. 50-51. These record-keeping requirements are limited in the case of small and medium-sized enterprises (fewer than 250 employees), "unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data [...] or personal data relating to criminal convications or offences..." *Id.*, art 30(5), p. 51.

A. Data Protection Impact Assessments (DPIAs)

The GDPR, in its Article 35[55], would add the requirement of conducting a data protection impact assessment (DPIA) regarding the impact of proposed processing operations in certain circumstances. We will begin our discussion by detailing the requirement that a DPIA be conducted in the final GDPR, Commission Draft and the Council Draft, prior to discussing the elements the DPIA will cover in the GDPR, and its differences with these two GDPR Drafts, and will conclude by discussing the slightly different lifecycle data protection management that had been proposed in the Parliament Draft, but ultimately not retained by the European legislators.

1. DPIA *Requirement* in the GDPR

In the final GDPR instrument, this requirement would apply where "a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons[56]." This develops further, and in a way that focuses more on the level of risk – a "high risk" – the concept already set out in the Commission Draft, where this requirement would have applied where processing operations "present *specific risks* to the rights and freedoms of data subjects by virtue of their nature, their scope or their purpose[57]" (emphasis added). Nonetheless, the Commission Draft indicates examples of what qualified as presenting "specific risks," involving processing of what are generally considered special categories of, or sensitive, data[58].

The Council Draft, which was closer to the final GDPR text on this point, is more specific here, providing that a controller shall conduct a DPIA prior to carrying out processing:

> [w]here a type of processing in particular taking new technologies, and taking into account the nature, scope, context and purposes of the processing, is

55 GDPR, *supra*, note 15, art. 35, p. 53-54.
56 *Id.*, art. 35(1), p. 53.
57 Commission Draft, *supra*, note 19, art. 33(1).
58 *Id.*, art. 33(2), p. 52.

> likely to result in a high risk for the rights and freedoms of individuals, such as *discrimination, identity theft or fraud, financial loss, damage to the reputation, unauthorized reversal of pseudonymisation, loss of confidentiality of data protected by personal secrecy or any other significant economic or social disadvantage* ... (emphasis added)[59]

The DPO, where designated, would be consulted under the GDPR when carrying out the DPIA[60].

This concept of "high risk" will be discussed again in the section on data breach notifications (Section II D). It should be noted that the concept of high risk (and DPIA) was slated in its priority 3 as an area for WP 29 to provide guidance to help controllers and processors get ready for entry into force of the GDPR[61], perhaps because of the difficulty or ambiguity of the concept – which may differ culturally from that in North America, for instance, where economic concerns relating to identity theft may be predominant. Companies should consult the April 2017 guidelines issued by WP 29 in the context of DPIAs, for use in determining whether processing is "likely to result in a high risk" for the purposes of the GDPR[62]. In any event, firms will need to come to understand their obligations here, and to train staff in order to ensure compliance.

Each of the Commission Draft and the Council Draft then set out examples of when a DPIA would be required, due to specific risks of processing (e.g., large-scale monitoring using optic-electronic devices[63], systematic and extensive evaluation of personal aspects relating to natural

---

59 Council Draft, *supra*, note 22, art. 33(1).

60 GDPR, *supra*, note 15, art. 35(2), p. 53.

61 European Union, *Article 29 Data Protection Working Party*, *Statement on the 2016 action plan for the implementation of the General Data Protection Regulation (GDPR)* (WP 236), February 2, 2016, online: <ec.europa.eu/justice/data-protection/article-29/documentation/.../2016/wp236_en.pdf> (consulted on September 15, 2017).

62 European Union, 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*, April 4, 2017, online: <http://ec.europa.eu/newsroom/document.cfm?doc_id=44137> (consulted on September 26, 2017).

63 Council Draft, *supra*, note 22, art. 33(2)(c).

persons[64], processing of biometric data[65], etc.), although there are differences in the two lists.

The final GDPR adopts the requirement for a DPIA where profiling is concerned[66], also where there is large scale processing of special categories of (or sensitive) data, which include personal data that reveal race or ethnic origins, political opinions, religious or philosophical beliefs, trade union membership, biometric and genetic data, health data, data regarding sexual life or orientation, or for data relating to criminal convictions or offenses[67]. (Where the term "on a large scale" is used, we can infer an attempt by legislators to take a risk-based approach.) The GDPR provides for the supervisory authority to "establish and make public a list of the kind of processing operations which are subject to the requirement" for a DPIA[68], and may also make a list of operations for which no DPIA is required[69].

2. Elements of a DPIA under the GDPR

The GDPR requires the following elements in a DPIA[70]:

- A systematic description of the processing;
- Evaluation or assessment of the respective risks referred to in paragraph 1 above; and
- Measures to address the risk (including safeguards, security measures, and data protection compliance assurance mechanisms).

In addition, the GDPR includes the views of data subjects or their representatives in the DPIA, "where appropriate," without prejudicing the "protection of commercial or public interests or the security of the

64 *Id.*, art. 33(2)(a); and Commission Draft, *supra*, note 19, art. 2(a). Both of these provisions are aimed at profiling, even if the Commission Draft does not specifically use such term.

65 Commission Draft, *supra*, note 19, art. 33(2)(d); and Council Draft, *supra*, note 22, art. 33(2)(b).

66 GDPR, *supra*, note 15, art. 35(3)(a), p. 53.

67 *Id.*, art. 35(3)(b), p. 53. The list of special categories of data is furnished in *id.*, art. 9(1), p. 38.

68 *Id.*, art. 35(4), p. 53.

69 *Id.*, art. 35(5), p. 53.

70 *Id.*, art. 35(7), p. 54.

processing operations[71]." The GDPR also explicitly includes in the DPIA an assessment of the "necessity and proportionality of the processing operations in relation to the purposes[72]," thus borrowing a concept from the Parliament Draft's lifecycle management proposal.

B. Prior Consultation and Prior Authorization

The GDPR provides that controllers should consult the supervisory authority prior to processing personal data in certain cases[73]. This obligation is limited to cases where a DPIA, "indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk[74]."

The requirement that this consultation be made will depend largely on determinations by data protection officers, supervisory authorities, or based on risk as determined in the DPIA. Under the GDPR:

> Member State law may require controllers to consult with, and obtain prior authorisation from, the supervisory authority in relation to processing by a controller for the performance of a task carried out by the controller in the public interest, including processing in relation to social protection and public health.[75]

This paragraph has the unfortunate result that divergence may then exist – divergence which was sought to be avoided by having a regulation rather than a directive as the European legislative instrument for reform – among the various Member States' legislation in how this issue is handled, however narrow the issue may be.

C. Data Protection Officers (DPOs)

One additional way in which the GDPR will impose internal compliance mechanisms for companies is through the requirement that certain companies (controllers and/or processors) engage a data protection

71 *Id.*, art. 35(9), p. 54, Commission Draft, *supra*, note 19, art. 33(4); and Council Draft, *supra*, note 22, art. 33(4), respectively.

72 *Id.*, art. 35(7)(b), p. 54.

73 See: *Id.*, art. 36(1), p. 54.

74 *Id.* This closely tracks a change made in the Council Draft, *supra*, note 22, art. 34(2).

75 GDPR, *supra*, note 15, art. 36(5), p. 55.

officer (DPO), who may be internal or external, but whose work would have an effect on the firm. First we will explore the GDPR requirements for engaging a DPO, after which we will place these in the context of present Member State law, prior to discussing the role of DPOs under the GDPR.

1. GDPR Requirements for Designating a DPO

The requirements vary according to the draft of the proposed GDPR considered, although the final GDPR takes a risk-based view and focuses on cases where personal data processing is a core activity of a controller or processor. If a controller or processor has as its core activities either (a) "processing operations which, by virtue of the nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale[76]"; or (b) "processing on a large scale of special categories of data [...] and personal data relating to criminal convictions and offences[77]," then there will be a requirement to designate a DPO. In addition, processing by a public authority or body (other than courts "acting in their judicial capacity"), requires designation of a DPO[78]. Generally speaking, then, we see that SMEs may be excluded from these requirements which focus on core activities but also processing done on a "large scale." This alleviates some of the concerns expressed regarding prior GDPR Drafts.

For example, in the Commission Draft, companies would have been required to designate a DPO in the following cases:

(a) the processing is carried out by a public authority or body; or

(b) the processing is carried out by an enterprise employing 250 persons or more; or

(c) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes require regular and systematic monitoring of data subjects.[79]

This approach, in so far as it concerns private companies, combines a numerical threshold (250 or more employees) and a risk basis (regular and

76 *Id.*, art. 37(1)(b), p. 55.
77 *Id.*, art. 37(1)(c), p. 55.
78 *Id.*, art. 37(1)(a), p. 55.
79 Commission Draft, *supra*, note 19, art. 35(1).

systematic monitoring of data subjects). However, voices were raised against this proposal to the extent that it might cause an unfair burden on SMEs, that the threshold of 250 employees was too low, and that a more risk-based approach should be adopted. The Article 29 Data Protection Working Party (WP 29), an EU advisory group which includes representatives from Member State data protection authorities, cautioned, however, that while obligations should be scalable to the controller and the relevant processing activity:

> Compliance should never be a box-ticking exercise, but should really be about ensuring that personal data is sufficiently protected. How this is done may differ per controller. This difference however, is not only dependent on the size of the controller, or on the amount of processing operations it carries out, but is also dependent for example on the nature of the processing and the categories of data it processes. Basing exceptions on quantitative qualifiers risks excluding companies from certain obligations that are actually of vital importance. Data subjects should have the same level of protection, regardless of the size of the organization or the amount of data it processes. Therefore the Working Party feels that all controllers must act in compliance with the law, though this can be done in a scalable manner.[80]

In the light of this statement, the GDPR's provisions seem an improvement over the original Commission Draft in that they focus on the categories of data being processed, and do not provide strict quantitative qualifiers.

Before the final GDPR, the Parliament Draft had shifted the focus from the number of employees of the data controller to the number of data subjects whose data was being processed (more than 5000 data subjects in any consecutive 12-month period)[81]. However, this would have still encountered WP 29's admonition against quantitative qualifiers. In addition, the Parliament Draft added a provision to require that a DPO be designated where sensitive data is being processed, more in line with WP 29's focus on categories of data being processed:

---

[80] European Union, *Article 29 Data Protection Working Party*, *Statement of the Working Party on current discussions regarding the data protection reform package*, February 27, 2013, online: <ec.europa.eu/.../data-protection/.../20130227_statement_dp_reform_package_en.pdf> (consulted on September 15, 2017).

[81] Parliament Draft, *supra*, note 20, art. 35(1)(b).

(d) the core activities of the controller or the processor consist of processing special categories of data pursuant to Article 9(1), location data or data on children or employees in large scale filing systems.[82].

The Parliament Draft may thus be seen as more risk-based in that it provides for requirements of a DPO where there is large-scale processing of personal data, or where sensitive data (in the European sense, and called "special categories of data"), or location data (which allows data subjects to be tracked in their movements), or the data of vulnerable or subordinate parties – children and employees, are processed.

The final GDPR, like the Commission Draft and the Council Draft, allows for the appointment of a single DPO for a group of undertakings, thus mutualizing this effort[83]. The Parliament Draft provided the possibility of the appointment of a "main responsible" DPO by a group of undertakings, provided that he or she is "easily accessible from each establishment[84]." The final GDPR provides that the DPO should have expert knowledge of data protection law and practice[85], and not have any conflicts of interest that result from any other tasks or duties[86]. Data subjects may contact the DPO "with regard to all issues related to the processing of their personal data" and for the exercising of their rights[87]. Without detailing them, similar provisions existed in the GDPR Drafts.

The final GDPR, like the Council Draft before it, breaks with the other GDPR Drafts in providing that Member State law may require designation of a DPO in other cases (although it should be noted that the Council Draft did not prescribe any specific cases when a DPO was required to be designated, thereby leaving the issue to the Member States)[88]. This may be considered a concession to Member States, as they already have varying DPO provisions, as discussed immediately below. Thus, similarly to the case of prior authorization under the GDPR, discussed above, the benefit of the unified legislation provided by a regulation is discarded, and one is

82 *Id.*, art. 35(1)(d).
83 GDPR, *supra*, note 15, art. 37(2), p. 55; Commission Draft, *supra*, note 19, art. 35(2); Council Draft, *supra*, note 22, art. 35(2).
84 Parliament Draft, *supra*, note 20, art. 35(2).
85 GDPR, *supra*, note 15, art. 37(5), p. 55.
86 *Id.*, art. 38(6), p. 56.
87 *Id.* art. 38(4), p. 56.
88 *Id.*, art. 37(4), p. 55; and Council Draft, *supra*, note 22, art. 35(1).

referred back to Member State law to determine if and when a DPO is required, in cases other than those provided for by the GDPR.

2. Examples of DPOs or Their Equivalent under Current Member State Law

Although the concept of DPOs is not new, today certain jurisdictions have them as an optional choice, which allows companies to lessen administrative burdens. This is explicitly provided for in the DP Directive, which provides that:

> Member States may provide for the simplification of or exemption from notification only in the following cases and under the following conditions:
>
> [...]
>
> – where the controller, in compliance with the national law which governs him, appoints a personal data protection official, responsible in particular:
>
> – for ensuring in an independent manner the internal application of the national provisions taken pursuant to this Directive
>
> – for keeping the register of processing operations carried out by the controller,[89]
>
> thereby ensuring that the rights and freedoms of the data subjects are unlikely to be adversely affected by the processing operations.

For example, in France companies may use a personal data protection officer ("correspondant à la protection des données personnelles," commonly known by the abbreviation for its prior name – "correspondant informatique et libertés" — "CIL") to serve this role. Under the current French Data Protection Act, the appointment of such an officer allows for an exemption from certain formalities:

> Processing for which the data controller has appointed a personal data protection officer ["Correspondant à la protection des données personnelles"] charged with ensuring, in an independent manner, compliance with the obligations provided for in this Act shall be exempted from the formalities provided for in Articles 23 [notification] and 24 [simplified notification], except where a transfer of personal data to a State that is not a Member State of the European Community is envisaged.[90]

---

89 DP Directive, *supra*, note 11, art. 18(2), p. 44.

90 *Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés*, *supra*, note 11, art. 22 (III).

Thus, companies are not under constraint to have a DPO under current data protection law in France, but rather are given an incentive to do so. Under the GDPR this will change to become a requirement, in the cases provided for in it.

It should be noted that one current example of an exception to this rule of optional appointment is contained in the German Federal Data Protection Law (FDPA) under which the appointment of a "Data protection official" may be mandatory for firms with ten or more employees involved in the automated processing of personal data:

> Public and private bodies which process personal data automatically shall appoint in writing a data protection official. Private bodies are obliged to appoint such an officer within one month of commencing their activities. The same shall apply where personal data are processed by other means and at least 20 persons are permanently employed for this purpose. The first and second sentences above shall not apply to private bodies which generally deploy a maximum of nine employees to carry out the automatic processing of personal data on an ongoing basis. In so far as the structure of a public body requires, the appointment of one data protection official for several areas shall be sufficient. In so far as private bodies carry out automated processing operations which are subject to prior checking or process personal data in the course of business for the purposes of transfer, anonymized transfer, or market or opinion research, they are to appoint a data protection official irrespective of the number of persons deployed to carry out automatic processing.[91]

A recent report of a decision of the Bavarian Data Protection Agency (BayLDA) is instructive regarding DPOs. Current interpretation of the FDPA indicates that the required reliability and independence of the DPO must include not having other duties that conflict with the DPO's monitoring obligations under the FDPA. The BayLDA found such a conflict of interest in a case where an appointed internal DPO also acted as the IT manager of a company, because in essence the DPO would have to monitor himself in his other role in order to ensure compliance with the FDPA. BayLDA requests for appointment of a new DPO went unheeded, resulting in the company being fined. According to the report, "conflicts of

[91] Bundesdatenschutzgesetz (BDSG), *Federal Data Protection Act*, January 14, 2003, as amended by art. 1 of the Act of August 14, 2009, online: <http://www.gesetze-im-internet.de/englisch_bdsg/englisch_bdsg.html> (consulted on September 15, 2017), art. 4f(1).

interest could also be seen if the DPO is the head of other departments that are heavily involved in the processing of personal data such as HR, legal, or marketing."[92] This case is interesting as it foreshadows the application of the GDPR requirement that a DPO not have any conflict of interest, discussed in paragraph 1 above.

One regulator commenting on the situation of Germany is reported to have stated that the DPO model has contributed to a "culture of data protection" there:

> the combination of the German adoption of the DPO model, the increasing power of that role, the diversity of national and state regulators and the privacy experts who work in them, and the empowerment of a variety of stakeholders in the field, Germany has created a "culture of data protection," where data protection has become "a business model."[93]

The question remains, under the GDPR will this be transposable elsewhere?

3. Role of a DPO under the GDPR: Organization and Tasks

The GDPR details the position of the DPO – the officer at the heart of compliance efforts in firms required to appoint one – in its Article 38. It specifies that the controller and the processor:

> [...] shall ensure that the data protection officer is involved, properly and in a timely manner, in all issues which relate to the protection of personal data.[94]

In performing his or her duties the DPO acts independently. As such he or she reports directly to the "highest management level[95]." Thus the

---

92 Julia Kaufmann and Jan-Philipp Guenther, «Germany: Data Protection Officer must not have a conflict of interests», *GlobalComplianceNews* (Baker and McKenzie), November 21, 2016, online: <https://globalcompliancenews.com/germany-data-protection-officer-conflict-of-interest-20161121/?utm_content=41649193&utm_medium=social&utm_source=twitter> (consulted on September 15, 2017). For a press release on this case (in german), see: Baylda, Press release, October 20, 2016, online: <https://www.lda.bayern.de/media/pm2016_08.pdf> (consulted on September 15, 2017).

93 Kenneth A. Bamberger and Deirdre K. Mulligan, *Privacy on the Ground: Driving Corporate Behavior in the United States and Europe*, The MIT Press, Cambridge, Massachusetts, 2015, p. 216.

94 GDPR, *supra*, note 15, art. 38(1), p. 55.

95 *Id.*, art. 38(3), p. 56.

GDPR anticipates internal reporting lines for the DPO within private firms that are controllers or processors subject to the requirement of designating a DPO.

DPOs are bound by secrecy or confidentiality "concerning the performance of his or her tasks[96], and a DPO shall not be penalized or dismissed for performing his or her tasks[97].

The DPO's tasks are set out in Article 39 of the GDPR, which in many ways resembles the Council Draft, in which there were perhaps fewer tasks set out than in the other GDPR Drafts, but the final GDPR (like the Commission Draft and Parliament Draft before it) indicates that the list is the minimum required by adding the phrase "at least[98]".

The DPO is to inform and advise the controller or the processor of its obligations under the GDPR[99]. The Commission Draft and the Parliament Draft had also provided that the DPO is also "to document this activity and the responses received[100]," a provision that was not retained in the final GDPR.

The DPO is also to monitor compliance with the GDPR, including awareness-raising and the training of staff and related audits[101]. The Commission Draft and the Parliament Draft also refer to the monitoring of the GDPR's requirements related to the following:

> [...] data protection by design, data protection by default and data security and to the information of data subjects and their requests in exercising their rights under [the GDPR].[102]

These references were not included in the final GDPR.

The Commission Draft and the Parliament Draft had provided that where there were documentation (record-keeping) requirements under the

96 *Id.*, art. 38(5), p. 56.
97 *Id.*, art. 38(3), p. 56.
98 *Id.*, art. 39(1), p. 56.
99 *Id.*, art. 39(1)(a), p. 56.
100 Commission Draft, *supra*, note 19, art. 37(1)(a); Parliament Draft, *supra*, note 20, art. 37(1)(a).
101 GDPR, *supra*, note 15, art. 39(1)(b), p. 56.
102 Commission Draft, *supra*, note 19, art. 37(1)(c); Parliament Draft, *supra*, note 20, art. 37(1)(c).

GDPR, the DPO was to ensure that the documentation is maintained[103], and, in addition, DPOs are to monitor "documentation, notification and communication of personal data breaches[104]," although these provisions are omitted in the final GDPR. Under the GDPR, the DPO is to cooperate with the supervisory authorities[105] and to act as the contact point with it[106].

Regarding DPIAs, which we have discussed above, the GDPR provides that DPOs are to monitor their performance, and, incorporating an addition from the Council Draft, where requested also provide advice as regards DPIAs[107].

4. DPOs in Practice: Intentions and Differences from Present

According to the IAPP-EY Annual Privacy Governance Report 2016, 35% of respondents to a recent survey of privacy professionals who believe their company will fall within the GDPR's scope report that their company will be appointing a DPO, and 16% multiple DPOs. The role of the DPO is seen to "differ in meaningful ways from the more strategic role played by the modern Chief Privacy Officer," as the DPOs will serve as "internal regulators and be responsive directly to data subjects." The report also compares the DPO's functions as "ombudsman-style roles."[108]

D. Data Breach Notifications

Unlike many North American jurisdictions[109], there are no European-wide obligations for notifying data breaches (although certain Member States, such as Germany and Austria, may provide national rules[110]), except, since relatively recently, with respect to providers of electro-

103 Commission Draft, *supra*, note 19, art. 28; Parliament Draft, *supra*, note 20, art. 31.

104 Commission Draft, *id.*, art. 37(1)(e); Parliament Draft, *id.*, art. 37(1)(e).

105 GDPR, *supra*, note 15, art. 39(1)(d), p. 56.

106 *Id.*, art. 39(1)(e), p. 56.

107 *Id.*, art. 39(1)(c), p. 56.

108 IAPP, *supra*, note 51, p. xi.

109 In the United States, for example, 47 out of the 50 States have data breach notification laws. National Conference of State Legislatures (NCSL), *Security Breach Notification Laws*, January 4, 2016, online: <http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx> (consulted on September 15, 2017).

110 J. Black and M. Dunne, *supra*, note 1, p. 159, at 171.

nic-communications services to the public (such as mobile telephone operators). This gap in data protection is discussed in the recitals in an amending directive to the EU e-Privacy Directive (Directive 2002/58/EC):

> The data breach notification requirements contained in Directive 2002/58/EC (Directive on privacy and electronic communications) provide a structure for notifying the competent authorities and individuals concerned when personal data has nevertheless been compromised. Those notification requirements are limited to security breaches which occur in the electronic communications sector. However, the notification of security breaches reflects the general interest of citizens in being informed of security failures which could result in their personal data being lost or otherwise compromised, as well as of available or advisable precautions that they could take in order to minimise the possible economic loss or social harm that could result from such failures. The interest of users in being notified is clearly not limited to the electronic communications sector, and therefore explicit, mandatory notification requirements applicable to all sectors should be introduced at Community level as a matter of priority. Pending a review to be carried out by the Commission of all relevant Community legislation in this field, the Commission, in consultation with the European Data Protection Supervisor, should take appropriate steps without delay to encourage the application throughout the Community of the principles embodied in the data breach notification rules contained in Directive 2002/58/EC (Directive on privacy and electronic communications), regardless of the sector, or the type, of data concerned.[111]

The GDPR fills this gap[112], and as a result companies that previously did not have to implement processes for communication in this regard will now have to do so. Companies will have to ensure that they have proper procedures in place in order to detect breaches and make notifications in a timely manner.

---

111 European Union, *Directive 2009/136/EC of the European Parliament and of the Council of 25 Nov. 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. (L337), December 18, 2009, online: <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32009L0136> (consulted on September 15, 2017), p. 11, at 19.

112 GDPR, *supra*, note 15, art. 33-34, p. 52-53.

Our discussion of data breach notifications begins by speaking of controller notification to the supervisory authority (1), then processor notification to controllers (2), and finally to communication to data subjects, when required (3). In each section we will set out the relevant time periods for action.

1. Controller to Supervisory Authority Notification

The principal obligation to notify personal data breaches is owed to the supervisory authority under the GDPR, and the controller is responsible for compliance[113], as is consistent with many obligations under the GDPR. This contrasts with, for example, U.S. State data breach notification statutes where, although the provisions vary State to State, typically there is a primary obligation "to notify the affected residents if their personal information was or may have been acquired by an authorized person" (there may be additional obligations to notify authorities or possibly the media, as well).[114] The requirement is for the notification to be made "without undue delay" – where feasible within 72 hours of becoming aware of it (outside of such period, the further delay shall be justified in a statement accompanying the notification), "unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons."[115] The notification must (i) describe the nature of the breach, if possible including categories and approximate numbers of data subjects and personal data records involved, and its likely consequences, (ii) provide DPO or other contact details, and (iii) describe measures taken or to be taken by the controller to address or lessen the impact of the breach.[116] The controller must document the breaches, so as to allow the supervisory authority to verify compliance.[117]

2. Processor to Controller Notification

The GDPR provides that processors are to notify the controller "without undue delay after becoming aware of a personal data breach."[118]

113 *Id.*, art 33, p. 52.
114 J. Black and M. Dunne, *supra*, note 1, p. 193.
115 GDPR, *supra*, note 15, art. 33(1), p. 52.
116 *Id.*, art. 33(3), p. 52.
117 *Id.*, art. 33(5), p. 52.
118 *Id.*, art. 33(2), p. 52.

Obviously, this is necessary in order for the controller to be able to comply with its obligations when a processor is involved.

3. Communication to Data Subjects

Where a data breach is "likely to result in a high risk to the rights and freedoms of natural persons", there is an additional requirement to communicate the breach to the relevant data subject "without undue delay."[119] The notification shall include the information mentioned in clauses (ii) and (iii) of point 1 above, as well as a description in clear and plain language of the breach, and the likely consequences of the breach.[120] However, this notification is not required if the controller had applied "appropriate technical and organizational protection measures" (such as encryption) to the data subject to the breach, subsequent measures have been taken to ensure that the high risk mentioned above "is no longer likely to materialise," or would involve "disproportionate effect," in which latter case a public communication measure may be used to inform the data subjects.[121] In addition, the supervisory authority, "having considered the likelihood of the personal data breach resulting in a high risk," may require the controller to communicate a breach to the data subject.[122]

III. Incentives for Compliance

We have seen in Section II that the GDPR offers fewer administrative burdens in terms of filing requirements and through its provision of a single law throughout the EU – in the form of a regulation – but that the counterpart to this is the greater accountability of firms. Now we will see that the mechanism for encouraging compliance has two sides to it – an increase in sanctions for non-compliance (Section III A) and a taking into consideration of compliance measures in the establishment of eventual sanctions (Section III B). Together these measures provide powerful reasons for firms to develop strong compliance programs.

119 *Id.*, art. 34(1), p. 52.
120 *Id.*, art. 34(2), p. 53.
121 *Id.*, art. 34(3), p. 53.
122 *Id.*, art. 34(4), p. 53.

A. Increased Sanctions for Non-Compliance

Presently, sanctions for violation of current data protection law vary in the different EU member states. This can be seen in the recent enforcement action conducted by six EU member state data protection agencies regarding Google's revised privacy policy. Google's sanctions included, *inter alia*, a fine of €150,000 in France, and three fines for a total of €900,000 in Spain[123]. Likewise, the disparity was evident in the earlier Google Street View enforcement actions, with a fine of €100,000 in France, a settlement of €150,000 in Belgium, and in relative contrast, a fine of €1 million in the Netherlands[124]. However, the amounts of these fines seem small compared to the $22.5 million fine that the Federal Trade Commission applied in the settlement of a case against Google where the latter misrepresented facts regarding the placement of cookies on the computers of users of the Apple Safari web browser[125].

Importantly, the GDPR will substantially increase the amounts of fines for data protection violations, up to 4% of annual worldwide turnover of the preceding financial year in certain circumstances[126]. Certainly, such a high level of potential administrative fines merits taking measures to ensure compliance.

B. Compliance as a Tool to Avoid or Reduce Potential Fines

Firms may reduce their risk of seeing such high fines imposed upon them by taking measures intended to ensure compliance. For example, supervisory authorities, when deciding whether to impose fines and in determining their amount, are to give due regard to (i) "any action taken by the controller or processor to mitigate the damage suffered by data subjects"[127], (ii) the controller or the processor's degree of responsibility "taking

123 W. Gregory Voss, « European Union Data Privacy Law Developments », (2014/2015) 70 *Business Lawyer* 253, 255.

124 W. Gregory Voss and al., « Privacy, E-Commerce, and Data Security », (2012) 46 *International Lawyer* 97, 102-103.

125 United States, Federal Trade Commission, *Privacy Settlement is the Largest FTC Penalty Ever for Violation of a Commission Order*, online: <http://www.ftc.gov/news-events/press-releases/2012/08/google-will-pay-225-million-settle-ftc-charges-it-misrepresented> (consulted on September 15, 2017).

126 GDPR, *supra*, note 15, art. 83(5)-(6), p. 83.

127 *Id.*, art. 83(2)(c), p. 82.

into account technical and organizational measures implemented by them"[128], (iii) adherence to approved codes of conduct[129], among other factors. This is consistent with the provision contained in Article 24 of the GDPR, that "[a]dherence to approved codes of conduct [...] or approved certification mechanisms [...] may be used as an element by which to demonstrate compliance with the obligations of the controller."[130] However, in order to benefit from these possible means to reduction of sanctions, firms must adopt internal compliance mechanisms that will impact their internal organization. In this sense, a similarity with the U.S. Sentencing Guidelines, where the existence of an effective compliance and ethics program may serve as a mitigating factor in case of punishment,[131] exists, although the GDPR provisions involve administrative sanctions (in the form of fines) and the U.S. Sentencing Guidelines, criminal sentencing, instead.

Nonetheless, the following questions arising from the debate in the first EDPS-Ethics Advisory Group workshop were reported by Mr. Buttarelli: "Is compliance with the GDPR, or indeed any law supporting data protection or privacy, only about avoiding harm or fault? Does compliance offer protection to the individuals the law is designed to protect or does it simply mitigate risks for organizations?"; adding the comment, "The weighing up of harm and risk also involves an ethical assessment."[132]

*
* *

As we have seen, the GDPR will result in internal compliance mechanisms for firms, which will have a great deal of impact on their internal

128 *Id.*, art. 83(2)(d), p. 82.

129 *Id.*, art. 83(2)(j), p. 82.

130 *Id.*, art. 24(3), p. 47.

131 See, for example: United States, Sentencing Commission, *Guidelines Manual* (November 1, 2016), online: <http://www.ussc.gov/sites/default/files/pdf/guidelines-manual/2016/GLMFull.pdf> (consulted on September 15, 2017), § 8C2.5 (f)(1), p. 548. See also: *id.*, ch. 8, "Sentencing of Organizations: Introductory Commentary," third principle, p. 525: "[...] The two factors that mitigate the ultimate punishment of an organization are: (i) the existence of an effective compliance and ethics program; and (ii) self-reporting, cooperation, or acceptance of responsibility."

132 Giovanni Buttarelli, *An Ethical Approach to Fundamental Rights*, European Data Supervisor, Blog, December 1, 2016, online: <https://secure.edps.europa.eu/EDPSWEB/edps/site/mySite/An_ethical_approach_to_fundamental_rights> (consulted on September 15, 2017).

organization, whether this be in hiring of personnel (such as a DPO), in the time and organization necessary to conduct DPIAs, in permitting the rapid notification of data breaches, and in record-keeping to prove compliance, among other obligations. The stakes are high, not only in terms of confidence in firms, but also in terms of the stakes involved as non-compliance becomes potentially more expensive, with the substantial increase in fines provided for under the GDPR.

Firms and their counsel should take full advantage of the period from now until the date of application of the GDPR in 2018 in order to fully understand its provisions and to best organize in anticipation of that date. This may involve the designating and fully training a DPO, organizing personnel capable of conducting a DPIA (or hiring outside help to do so), providing for better record-keeping and improving communication means in order to comply with data breach notification requirements, among other actions. It most certainly will mean raising awareness about the GDPR and its requirements internally, including through seminars and other training.

While the models of data protection legislation on both sides of the Atlantic differ, the GDPR will require certain internal data protection compliance mechanisms and inspire others that may have similarities with compliance efforts in North America. The GDPR's provisions highlight the importance of a robust compliance program, building a culture of compliance, and helping keep firms on the right side of the law through awareness-raising, training, risk assessments and monitoring. The existence of a proper GDPR compliance program, like an effective compliance and ethics program under the U.S. Sentencing Guidelines, may serve to reduce punishment in the case of an eventual violation. However, as the EDPS said, "the GDPR reinforces the need for organisations to be accountable; what if we consider that accountability implies a responsibility to take ethical considerations into account as part of an organisation's corporation social responsibility?"[133] That interrogation merits further thought and research, taking into consideration the distinctive fundamental rights basis of data protection and privacy in the European Union, which is lacking in the United States.

[133] *Id.*