Bloomberg BNA

Privacy and Security Law Report®

The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law

BY CHRISTOPHER KUNER

I. Introduction

In the 18th century Immanuel Kant famously initiated a "Copernican revolution" in philosophy by shifting the understanding of reality away from external objects and toward the cognitive powers of the individual.[1] The European Commission's recent proposal for a General Data Protection Regulation[2] (the "Proposed Regulation") attempts a similar revolution in European data protection law by seeking to shift its focus away from paper-based, bureaucratic requirements and toward compliance in practice, harmonization of the law, and individual empowerment. Indeed, the Proposed Regulation represents the most significant potential change to European data protection law since adoption of the EU Data Protection Directive 95/46/EC[3] ("Directive 95/46") in 1998.

The Proposed Regulation is part of a package of measures (the "Proposal") issued on Jan. 25, 2012 that also includes a Communication outlining the Commission's strategy (the "Communication"),[4] a proposed directive ("the Proposed Directive") containing rules for data processing "with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties."[5] and various other documents.[6] The Directive, which would replace the current Council Framework Decision in the same area,[7] will not be discussed, with a few exceptions. Since the documents issued by the

[1] Immanuel Kant, *Kritik der reinen Vernunft* 28 (B XVI-XVIII) (Reclam-Verlag 2009).

[2] 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) 11/4 draft (including explanatory memorandum). Unless otherwise indicated, throughout this article the relevant provisions of the Proposed Regulation are indicated in parentheses after the text to which they refer.

Christopher Kuner is a partner with Hunton & Williams LLP in Brussels. This article is written in the author's personal capacity. The author is grateful for the valuable research assistance of Anna Pateraki and Anne Ruwet.

[3] Directive (EC) 95/46 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] OJ L281/31.

[4] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Safeguarding Privacy in a Connected World—A European Data Protection Framework for the 21st Century, COM(2012) 9/3 [hereinafter Communication].

[5] Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, COM(2012) 10/3, Article 1(1).

[6] The following other documents are included in the package: Report from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions based on Article 29(2) of the Council Framework Decision of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (including annex), COM(2012) 12 final; Impact assessment (including annexes) accompanying the Proposed Regulation and the Proposed Directive, SEC(2012) 72 final [hereinafter Impact assessment]; and Executive summary of the impact assessment, SEC(2012) 73 final [hereinafter Executive summary]. All the documents are available at http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm.

[7] Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal mat-

 ISSN 1538-3423

Commission are lengthy and highly complex, only selected provisions of the Regulation of the greatest potential interest to companies and the private sector will be analyzed here.

Completion of the EU legislative process is a politically charged undertaking that will likely take at least one to two years to complete,[8] and will require approval by the Council of the European Union and the European Parliament; the Proposed Regulation is to take effect two years after that. This lengthy process also makes it practically certain that there will be changes (potentially major ones) to the Proposal.

The Proposed Regulation would remake the data protection landscape in Europe by introducing far-reaching changes such as the following:

- The law would be largely harmonized among the EU member states, so that the provisions of the Regulation would apply EU-wide.
- Companies with operations in multiple EU member states would be subject to the jurisdiction of a single data protection authority, and the jurisdictional rules over data controllers outside the EU would be changed.
- The use of consent for legitimizing data processing would be significantly restricted.
- Certain bureaucratic requirements, such as notification of data processing to the data protection authorities (DPAs), would be eliminated, but other ones (such as to maintain extensive internal documentation about data processing) would be introduced.
- Companies with more than 250 employees would have to appoint a data protection officer.
- A number of new fundamental rights (such as the "right to be forgotten") would be introduced, as would requirements to use data protection "by design" and "by default."
- Regulators and affected individuals would have to be notified of data security breaches.
- There would be some simplification of the procedures for transferring personal data outside the European Union.
- Independence of the DPAs would be strengthened, and they would receive enhanced resources and enforcement powers, but much policymaking power would shift from the member states to the European Commission.
- Administrative fines for data protection violations could range up to 2 percent of a company's annual worldwide income.

These are just a few changes of greatest interest to companies, and are discussed in more detail below.

II. Background

On May 15, 2003, Directorate General Internal Market of the Commission (which had jurisdiction over data protection policymaking at that time) published its "First report on the implementation of the Data Protection Directive (95/46/EC),"[9] and on March 7, 2007, the Commission adopted a Communication concluding that the Directive should not be amended.[10] However, on Nov. 4, 2010, the Commission released another Communication[11] concluding that, while the core principles of Directive 95/46 were still valid, the Directive could no longer meet the challenges of rapid technological developments and globalization, and required revision. The Commission then engaged in extensive consultations, both public and private, with citizens' groups, businesses, DPAs, national governments, technical experts, NGOs, and other parties. In assessing the various options for reform, the Commission ultimately decided on the second of three policy options it was considering, consisting in the main of a thorough modernization of the legal framework.[12] On Nov. 29, 2011, DG Justice circulated within the Commission services a draft version of the Proposal, which was leaked widely.[13] The draft texts proved controversial within the Commission services, which led to several of them issuing negative opinions during the Commission interservice consultation procedure. Following the adoption of numerous changes and improvements to the texts, the final Proposal was released on Jan. 25, 2012.

One of the major reasons for the Commission's decision to rethink the EU data protection framework was the Treaty of Lisbon (Lisbon Treaty or Reform Treaty), which entered into force on Dec. 1, 2009,[14] and brought about major constitutional changes in the legal structure of the European Union. With regard to data protection, these include a mention in Article 16 of the Treaty on the Functioning of the European Union (TFEU) that everyone has a right to data protection;[15] elimination of the EU's "pillar" structure, meaning that from now on the same basic legal protections should apply to all types of data processing;[16] increased oversight of and participation in data protection policymaking by the European Parliament; mention of data protection as a fundamental right in the Charter of Fundamental Rights of the European Union;[17] and the obligation of the EU to accede to the European Convention on Human Rights.[18]

There had been a great deal of discussion as to whether the new instrument should take the form of a directive or a regulation. A regulation has general application and is directly applicable (i.e., it does not require

---

ters, [2008] OJ L350/60. *See* the Proposed Directive, Article 58(1), repealing the Council Framework Decision.

[8] The Commission's estimate that final agreement on the Proposal can be reached "by the end of 2012" can be regarded as highly optimistic. Communication *supra* note 4, at 12.

[9] Commission document COM(2003) 265 final.

[10] Communication from the Commission to the European Parliament and the Council on the follow-up of the Work Programme for better implementation of the Data Protection Directive, Commission document COM(2007) 87 final, at 9.

[11] European Commission, "A comprehensive approach on personal data protection in the European Union," COM(2010) 609 final (Nov. 4, 2010).

[12] *See* Executive summary*supra* note 6, at 8–9.

[13] Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), Version 56 (29/11/2011), http://statewatch.org/news/2011/dec/eu-com-draft-dp-reg-inter-service-consultation.pdf.

[14] Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community [2007] OJ C306/1.

[15] Consolidated version of the Treaty on the Functioning of the European Union (TFEU) [2010] OJ C83/47, Article 16(1) [hereinafter Treaty].

[16] *Id.*, Article 16(2).

[17] Charter of Fundamental Rights of the European Union [2010] OJ C83/2, Article 8.

[18] Treaty, *supra* note 15, at Article 6(2).

PVLR ISSN 1538-3423

implementation by EU member states), whereas a directive sets forth the results to be achieved, but leaves the means for achieving them largely up to implementation into national law by the member states.[19] One of the major complaints with Directive 95/46 has been the lack of harmonization, which is made possible by its status as a directive. In theory, the type of legal instrument used is not in itself determinative with regard to harmonization; for example, it is possible for a directive to leave little margin for member state implementation.[20] However, a regulation leads to a greater degree of harmonization, since it immediately becomes part of a national legal system, without the need for adoption of separate national legislation; has legal effect independent of national law; and overrides contrary national laws.[21]

But even a regulation cannot result in complete, 100 percent harmonization of all legal provisions affecting data protection, or totally eliminate the need to amend national laws. For example, member states may need to enact complementary legislation to deal with the effects of a regulation on their national legal systems. In addition, the Proposed Regulation would not harmonize issues governed by laws outside the area of data protection, such as the powers of works councils under national labor laws,[22] or laws governing freedom of expression.[23] Some provisions of the Proposed Regulation also seem to require a kind of national implementation: an example is Article 76(5), stating that "Member States shall ensure that court actions available under national law allow for the rapid adoption of measures including interim measures . . . ." The vague language of many provisions of the Proposed Regulation also means that some room for interpretation of them will remain. Thus, some degree of diversity among national systems can be expected in practice even once the Proposed Regulation comes into force.

Recital 10 of the Proposed Regulation states that its legal basis is to be found in Article 16(2) TFEU, meaning that it is to be adopted by the so-called "ordinary legislative procedure" under Article 294 TFEU.[24] Without going into further detail, this procedure foresees a complicated process of consultation between the Council and the European Parliament.[25] This process is likely to be politically contentious, since some member states may not like having their national data protection framework overridden by legislation from Brussels, and some individuals may also mistrust an EU regulation that replaces their national law. Concerns already are being voiced in Germany, where Johannes Masing, a judge on the German Federal Constitutional Court (*Bundesverfassungsgericht*), published an article in a leading German newspaper Jan. 9 arguing that a data protection regulation would violate the German constitution, since it would remove protections that have been created by the Court's jurisprudence and replace them with insufficient protections under EU law.[26] Some local German DPAs have also issued a press release expressing concerns about the legality of having the Commission assume certain supervisory functions traditionally exercised by the DPAs.[27] Based on past experience, at some point the German Federal Constitutional Court might well be asked to adjudicate the constitutionality of the Proposed Regulation, thus setting up a potential clash between EU law and German constitutional law. These sorts of concerns will likely be voiced in other member states as well, and it is possible that important changes might have to be made to the Proposal to take them into account.

III. Analysis of Key Provisions

Given the length and complexity of the Proposed Regulation, this article can only provide an overview of its most significant provisions. The analysis is structured based on its chapters, with the most important concepts and issues listed below the chapter title. The text discussed is that of the final text of the Proposed Regulation issued Jan. 25; in some cases, the final text is compared to the interservice draft (of Nov. 29, 2011), to show how it evolved. The reader should remember that, even though they are not legally binding, the recitals provide crucial clarification of many points in the text, and should be read together with it.

Chapter I: General Provisions

Subject Matter and Objectives—Material and Territorial Scope—Definitions

Article 3 of the Proposed Regulation contains the rules governing its territorial scope. It retains from Article 4 of Directive 95/46 the concept of "the processing of personal data in the context of the activities of an establishment" in the EU as the basic test for determining when EU data protection law applies (Article 3(1)). However, the Proposed Regulation goes on to make several significant changes with regard to jurisdiction. Under Article 3(2), data controllers not established in the EU may be subject to EU law when their processing activities are related to "the offering of goods or services" to data subjects residing in the EU, or to the monitoring of the behavior of EU residents; the abandonment of the "use of equipment in the EU" test contained in Article 4(1)(c) of Directive 95/46 as the criterion for jurisdiction over non-EU data controllers is welcome. The effect of these changes is to bring more non-EU-based companies offering services over the internet within the reach of EU law. The meaning of "monitor-

[19] *Id.*, Article 288.

[20] An example is the new EU Consumer Rights Directive. Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council [2011] OJ L304/64.

[21] *See* Paul Craig & Gráinne de Búrca, *EU Law: Text, Cases, and Materials* 105-06 (Oxford Univ. Press 5th ed. 2011).

[22] Note, however, that Article 82 of the Proposed Regulation encourages member states to adopt national rules governing data processing in the employment sector.

[23] Freedom of expression is largely left up to member states under Article 80.

[24] The relevant part of Article 16(2) reads: "The European Parliament and the Council, *acting in accordance with the ordinary legislative procedure*, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data . . . " (emphasis added).

[25] *See* Craig & de Búrca*supra* note 21, at 123-29.

[26] Johannes Masing, *Ein Abschied von den Grundrechten*, Süddeutsche Zeitung, Jan. 9, 2012, at 10.

[27] *See* press release by the DPAs of the German federal states of Rheinland-Pfalz and Hessen, Jan. 28, 2012, "Keine Datenschutzaufsicht durch die Kommission!," http://www.datenschutz.rlp.de/de/presseartikel.php?pm=pm2012012601.

ing" the behavior of EU residents seems to be linked to whether the non-EU data controller is creating "profiles" of them (Recital 21). The territorial scope of EU data protection law with regard to processing by non-EU data controllers is explicitly limited to individuals "residing" in the EU, but it is not explained whether such residence must be permanent or may only be temporary, and what protection, if any, would be enjoyed by individuals who may have a residence both inside and outside the EU. Indeed, the emphasis in this and other articles (e.g., Articles 41(2)(a) and 41(5)) on residence in the EU is surprising, given that the Proposed Regulation states elsewhere that its protections should apply regardless of nationality or residence (e.g., in Recitals 2 and 12).

The interservice version of these provisions based jurisdiction over non-EU data controllers on "directing activities" to EU residents or monitoring their behavior, using criteria articulated in the 2010 judgment of the European Court of Justice in the joined cases *Pammer* and *Alpenhof*,[28] but the final version has abandoned the criteria listed therein and substituted "the offering of good or services" for "directing activities." While the concept of "directing activities" via the internet has proved difficult to define, the *Alpenhof* decision did at least contain some concrete criteria upon which a determination could be based.[29] Given the uncertainty of interpreting the "offering of goods or services" and "monitoring the behavior of EU residents" tests, it is regrettable that, in this of all areas, there is no power for the Commission to issue a delegated or implementing act providing further clarification. The Proposed Regulation does not contain rules governing choice of law between the EU member states, since the fact that the rules are now harmonized largely removes the need for this. However, complete harmonization of the law is unlikely despite the enactment of a regulation, and so questions may still arise as to whether the law of a particular EU member state, or a member state's interpretation of the Proposed Regulation, applies in a specific case.

As mentioned above, one of the main changes to the data protection framework under the Lisbon Treaty and the accompanying instruments is the need to provide a harmonized regime also for data processing under the former "third pillar" of EU law (i.e., for matters involving law enforcement). Such matters are currently outside the scope of Directive 95/46;[30] while this does not mean that they are not covered by data protection rules, they are subject to a variety of different rules that have been adopted on an *ad hoc* basis and differ greatly. The easiest and cleanest way of dealing with this situation would have been to make law enforcement issues subject to the Proposed Regulation as well, especially since it generally covers data processing by public authorities,[31] but this proved politically impossible.

However, data processing by "competent authorities" (i.e., public authorities) for the purpose of preventing, investigating, detecting, or prosecuting criminal offenses or for executing criminal penalties is exempted from the scope of the Proposed Regulation, as are any activities falling outside the scope of EU law, "in particular concerning national security"; data processing by EU institutions; and data processing by member states that falls within the EU Common Foreign and Security Policy (Article 2(2)). Determination of whether the Proposed Regulation or the Proposed Directive applies to a particular act of data processing is presumably based on who was processing the data, so that if, for example, EU criminal justice authorities were seeking access to personal data held in a database by a private company, the Proposed Directive would be applicable. However, certain inconsistencies in the terminology used in the Proposed Directive and Regulation could lead to confusion. For example, the Proposed Directive only applies to data processing by "competent authorities," meaning EU criminal justice authorities.[32] However, Recital 87 of the Proposed Regulation also refers to international data transfers to "competent authorities," which in the context of international transfers only makes sense if the term means criminal justice authorities outside the EU; this point should be clarified. It is not clear which, if any, data protection rules would govern "national security," which is presumably left to national law. It is unfortunate that the Regulation does not cover data processing by the EU institutions, which would allow for an updating of the present EU Regulation 45/2001[33] covering data processing by the EU bodies.[34]

---

[28] Joined Cases C-585/08 and C-144/09 (Dec. 7, 2010). Recital 15 of the interservice version contained criteria to determine when targeting occurs that are taken from conclusion no. 2 of the Court's judgment.

[29] *Id.* at para. 93: "The following matters, the list of which is not exhaustive, are capable of constituting evidence from which it may be concluded that the trader's activity is directed to the Member State of the consumer's domicile, namely the international nature of the activity, mention of itineraries from other Member States for going to the place where the trader is established, use of a language or a currency other than the language or currency generally used in the Member State in which the trader is established with the possibility of making and confirming the reservation in that other language, mention of telephone numbers with an international code, outlay of expenditure on an internet referencing service in order to facilitate access to the trader's site or that of its intermediary by consumers domiciled in other Member States, use of a top-level domain name other than that of the Member State in which the trader is established, and mention of an international clientele composed of customers domiciled in various Member States."

[30] *See* Article 3(2) of Directive 95/46.

[31] *See* the Proposed Regulation, Article 4(5) and (6), defining both "controller" and "processor" (which are the entities with compliance responsibilities) to include public authorities and agencies.

[32] *See* explanatory memorandum, at 7, explaining that the phrase "competent authorities" is based on its use in Article 2(h) of the Council Framework Decision, where it is defined as "agencies or bodies established by legal acts adopted by the Council pursuant to Title VI of the Treaty on European Union, as well as police, customs, judicial and other competent authorities of the Member States . . . ."

[33] Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community, institutions and bodies and on the free movement of such data [2001] OJ L8/1.

[34] *See* European Data Protection Supervisor, "Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions—A comprehensive approach on personal data protection in the European Union" (Jan. 14, 2011), at para. 8, urging inclusion of data processing by EU institutions and bodies in the Commission's proposal.

 PVLR ISSN 1538-3423

The Proposed Regulation also excludes from its scope data processing by a natural person "without any gainful interest in the course of its own exclusively personal or natural or household activity" (Article 2(2)(d)). There has been concern among European data protection authorities and the European Commission that the current scope of the exemption under Article 3(2) of Directive 95/46 is too broad, since it could be construed to exempt from EU data protection law activities such as the processing of personal data by online social networks.[35] The interservice version contained a further restriction stating that data processed for a personal or household activity were not covered by the exemption if they were "made accessible to an indefinite number of individuals," reflecting the judgment of the European Court of Justice in the case *Satamedia*,[36] but this was deleted in the final version. The definition of a "data subject" as an "identified *natural* person" (Article 4(1), emphasis added) implies that legal persons are not covered by the Proposed Regulation, a point which is confirmed by Recital 12.[37]

Important changes have been made to other definitions currently contained in Directive 95/46, which are set forth in Article 4 of the Proposed Regulation. In particular, the elements of the existing definition of "personal data" (in Article 2(a) of Directive 95/46) have been moved into the definition of "data subject," with certain changes. Article 4(1) implies that "online identifiers" such as internet protocol addresses and cookies are generally to be considered as personal data, but a sentence has been added to Recital 24 since the interservice version clarifying that "[i]dentification numbers, location data, online identifiers or other specific factors as such need not necessarily be considered as personal data in all circumstances." This clarification is welcome, given that an overly inclusive definition of personal data could effectively require data controllers to identify individuals in borderline cases so that they could comply with other legal requirements, and would thus be counterproductive. Thus, Article 10 specifies that data controllers do not need to identify a person just to comply with the provisions of the Proposed Regulation, and Recital 23 states that "the principles of data protection should not apply to data rendered anonymous in such a way that the data subject is no longer identifiable"; this provides powerful incentives for the use of anonymization techniques.

Highly significant also is the tightening of the definition of consent, which now must always be "explicit" (i.e., opt-in, see Article 4(8)). Together with other new rules on consent discussed later on, mandating the use of opt-in consent in all cases will have significant implications for companies engaged in e-commerce and online activities (e.g., by requiring an increased use of pop-up boxes and other mechanisms on websites that indicate an individual has affirmatively agreed to their personal data being processed).[38] At the same time, certain changes were introduced to Recital 25 since the interservice version to soften the consent requirements somewhat in the online context, such as stating that the giving of electronic consent should not be "unnecessarily disruptive," and that consent can be given by a "statement or a clear affirmative action." It seems that this would also allow actions such as downloading an application or playing an online game to constitute consent.

A number of new definitions are also introduced, including "personal data breach," "genetic data," "data concerning health," "binding corporate rules," "main establishment," and others. The Proposed Regulation defines a "child" as any person below 18 years (Article 4(18)), and introduces a number of protections when the personal data of children are processed (e.g., Articles 8, 33(2)(d), and 52(2)). However, a revision introduced during the interservice consultation resulted in the age at which personal data of a child may not be processed online without consent of the parent or custodian being lowered to 13 years (Article 8(1)).

Chapter II: Principles

Data Processing Principles—Lawfulness of Processing—Consent—Data of a Child—Sensitive Data—Processing Not Allowing Identification

The Proposed Regulation foresees a strengthening of the general conditions for data processing. This is reflected first of all in Article 5, which is an amended version of Article 6 of Directive 95/46. The basic principles of that article have been retained, with some notable additions. Article 5(c) provides a more explicit expression of the "data minimization" principle than is currently contained in Directive 95/46, and will require companies to limit much more strictly the amount of data they collect. Article 5(f) strengthens the accountability of data controllers by requiring that personal data be processed under the responsibility and liability of the controller, who also is responsible for compliance with the Proposed Regulation. However, this provision does not reflect the fact that other articles foresee compliance responsibility by the data processor as well (such as Articles 26, 31, and 34(1)).

Article 6 (corresponding to Article 7 of Directive 95/46) contains several important changes to the legal bases for data processing. Article 6(3) states that any data processing may only be based on EU law or member state law; this will clarify that the law of a non-EU country may not serve as the legal basis for processing. Recital 39 states that the processing of data strictly necessary to ensure network and information security is to be considered a "legitimate interest" of the data controller, thus allowing the balancing of interests tests to legalize such activities. Since it is often difficult to find a clear legal basis for the processing of personal data for network and IT security purposes, this clarification

[35] *See* Article 29 Working Party, "The Future of Privacy" (WP 168, Dec. 1, 2009), at para. 71, stating that the current exemption under Article 3(2) leads to "a lack of safeguards which may need to be addressed," Article 3(2) currently exempts data processing "by a natural person in the course of a purely personal or household activity."

[36] Case C-73/07 [2008] ECR I-09831, where the Court found at para. 44 that the exemption contained in Article 3(2) of Directive 95/46 for personal or household processing only relates to "activities which are carried out in the course of private or family life of individuals," and thus did not apply to activities of private companies that were intended to make the data collected accessible to an unrestricted number of people.

[37] Recital 12 states that legal persons "should not be able to claim the protection of this Regulation."

[38] *See* Recital 25, which provides that consent should be "freely given . . . either by a statement or by a clear affirmative action by the data subject . . . including by ticking a box when visiting an Internet website . . . ."

is a welcome step that should facilitate activities to improve the level of information security in the EU. The Commission is to adopt a number of delegated acts under this article, including one to clarify use of the "balancing of interests" test for data processing under Article 6(1)(f); given the complexity of this issue, the permissibility of which can often only be judged based on the facts of a particular case, it is unclear how the Commission can produce guidance that is both authoritative and specific enough to be useful. A requirement that sending direct marketing requires the consent (i.e., opt-in consent) of the recipient, which was contained in the interservice version, was deleted from the final version; Article 19 now only requires a right to object for the sending of direct marketing.

The limitations on the use of consent contained in Article 7 are highly significant, given the widespread use of consent as a legal basis for data processing in both the private and public sectors. Under Article 7(1), data controllers bear the burden of proof in showing that data subjects consented to the processing of their personal data. Under Article 7(4), the use of consent is not allowed "where there is a significant imbalance between the position of the data subject and the controller"; Recital 34 clarifies that this applies especially "where personal data are processed by the employer of employees' personal data in the employment context." Thus, the use of consent as a legal basis for processing employee data will be made more difficult.

Finally, Article 9(1) expands the definition of sensitive data somewhat to also include genetic data and data concerning "criminal convictions or related security measures." The processing of such criminal data is possible only under restrictive conditions based on Article 9(2)(j), though deletion of the word "offenses" from the definition of sensitive data, together with reformulation of the clause during the interservice process, should make it somewhat easier than was the case under the interservice version for companies to comply with legal obligations, such as those under national laws implementing the third EU anti-money laundering and terrorist financing directive (2005/60/EC).[39]

Chapter III: Rights of the Data Subject

TRANSPARENCY—PROCEDURES AND MECHANISMS FOR EXERCISING DATA SUBJECT RIGHTS—INFORMATION RIGHTS—RIGHT OF ACCESS—RECTIFICATION—RIGHT TO BE FORGOTTEN AND ERASURE—DATA PORTABILITY—OBJECTION—PROFILING—RESTRICTIONS

The Proposed Regulation aims to increase the transparency of data processing, and to this end imposes stricter informational and transparency obligations on data controllers. Some of these requirements are phrased in broad terms (e.g., Article 11, mandating that data controllers have "transparent and easily accessible policies with regard to the processing of personal data and for the exercise of data subjects' rights"), and others in quite detailed form (e.g., Article 14, which contains a list of the types of information that data subjects must be provided with). Furthermore, data controllers are obliged to implement detailed procedures for allowing individuals to exercise their rights (Article 12). These requirements will cause many companies to review and revise their privacy policies and informational practices. The Commission is empowered to adopt acts setting forth standard forms and procedures for individuals to exercise their rights (e.g., Article 12(6)), which should eliminate the need to follow separate procedures in individual member states.

Article 17, dealing with the "right to be forgotten and to erasure," is likely to be one of the most controversial provisions of the Proposed Regulation. It seems to be an extension of the existing right currently contained in Article 12 of Directive 95/46 to have data erased, and it is not clear why it was necessary to create a new right under a new name. This provision was amended during the interservice consultation to limit it somewhat; in particular, in the previous version controllers who made data public had a duty to ensure the erasure of any internet link to or copy of the data, which would have made them responsible for policing the entire internet. This duty has now been limited to informing third parties processing the data that the data subject has requested that they be erased (Article 17(2)), and such duty has been limited to what is possible and does not involve a disproportionate effort (Article 13). During the interservice consultation, it was clarified in Article 2(3) that the liability rules of intermediary service providers contained in Articles 12–15 of the E-Commerce Directive[40] continue to apply, so that they should limit the liability of such providers with regard to the right to be forgotten as well. It is unlikely that data controllers will be able to make on their own complex determinations about balancing the right to be forgotten against rights such as free expression (Article 17(3)), and whether data are to be erased (under Article 17(3)) or the processing of them is to be restricted (Article 17(4)), as is foreseen in the text. As currently formulated, Article 17 will likely prove difficult to apply in practice, and may have a chilling effect on use of the internet in the EU. A new "right to data portability" that also would be created (Article 18) is designed to allow individuals to change online services more easily by giving them the right to obtain a copy of their data from their service provider.

Article 20 of the Proposed Regulation regulates the use of "profiling," and is based both on Article 15(1) of Directive 95/46 and on the recent Council of Europe Recommendation on profiling.[41] "Profiling" is defined as "a measure which produces legal effects concerning this natural person or significantly affects this natural person, and which is based solely on automated processing intended to evaluate certain personal aspects relating to this natural person or to analyse or predict in particular the natural person's performance at work, economic situation, location, health, personal preferences, reliability or behaviour" (Article 20(1)). In fact, "profiling" as used here would seem to cover many routine data processing operations that may also benefit the individuals concerned, such as, for example, routine operations to evaluate the performance of employees.

[39] Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing [2005] OJ L309/15.

[40] Directive (EC) 2000/31 of the European Parliament and the Council of 8 June 2000 on certain legal aspects of electronic commerce in the Internal Market [2000] OJ L178/1.

[41] Council of Europe, Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling (Nov. 23, 2010).

PVLR ISSN 1538-3423

Article 20(2) then places severe restrictions on the way that such profiling may be conducted, which will likely cause many companies to reevaluate their data processing practices, particularly in the online sphere. Much of the terminology used in this article is unclear and likely to be difficult to implement in practice.

The Proposed Regulation states that data protection is not an absolute right, but must be considered in relation to its function in society, and must be balanced with other fundamental rights (Recital 139).[42] The explanatory memorandum to the Proposed Regulation lists the rights to property and in particular the protection of intellectual property as among the fundamental rights enshrined in the EU Charter of Fundamental Rights,[43] a fact which has also been emphasized in the case law of the European Court of Justice.[44] Unfortunately, Recital 139 fails to include these two rights among those that have to be balanced against the right to data protection, an omission that should be rectified. Under Article 21, a number of rights (including the rights of information, access, rectification, erasure, data portability, and the right to object; protections against profiling; and the communication of a data breach to individuals) may be limited to safeguard certain public interests (such as public security, important economic or financial interests, various regulatory functions, and others), using criteria drawn from interpretations of the European Convention on Human Rights by the European Court of Human Rights.[45] This article provides some flexibility in case of collisions between data protection rights and other fundamental rights and interests, and does so in a more balanced and proportionate way than Article 3(2) of Directive 95/46, which provides a complete exemption from the Directive for data processing in areas such as public security. At the same time, the exemptions seem rather broad and ill-defined, which could lead to a lack of harmonization and excessive use of them by member states.

Chapter IV: Controller and Processor

Responsibility of controllers—Data protection by design and by default—Joint controllers—Representatives of non-EU controllers—Data processors—Processing under the authority of the controller and processor—Documentation—Cooperation with DPAs—Data security—Security breach notification—Data protection impact assessments—Prior authorisation—Data protection officers—Codes of conduct—Certification

This is a highly complex and diverse section, covering many different topics, but with a common theme of enhancing the responsibility and compliance obligations of data controllers and processors.

Article 22 imposes duties of responsibility and accountability on data controllers, and mandates that compliance measures be independently verified (Article 22(3)), though the use of "independent internal or external auditors" is only required if this is "proportionate." The concept of accountability seems to include the measures listed in Article 22(2), namely keeping documentation of data processing; implementing data security requirements; performing data protection impact assessments; complying with requirements for prior authorization by or in consultation with the DPAs; and designating a DPO. An earlier provision requiring that data protection compliance be mentioned in annual corporate reports and other documents that companies are required to file by law was deleted following the interservice consultation. Article 23 requires that data controllers implement "appropriate 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" (Article 23(1), data protection by design), and that measures are implemented "by default" so that "only those personal data are processed which are necessary for each specific purpose of the processing" (Article 23(2), data protection by default). The meaning of the phrase "by default" is unclear, but presumably it would mean that privacy-friendly features of products and services would have to be activated automatically when they are used (e.g., that certain settings in internet browsers are turned on from the time the browser is first used). Privacy by design and by default will have profound implications in particular for hardware and software companies, data processing service providers, and other companies that either produce products for the processing of personal data or that process data intensively. The details of what they mean in practice are to be set forth in delegated acts and technical standards issued by the Commission (Articles 23(3)–(4)).

The Proposed Regulation contains a provision dealing with joint data controllers (Article 24), which requires them to conclude an "arrangement" allocating data protection responsibility between them, which will require many companies to modify their commercial agreements. Article 26 also will have important implications for many outsourcing arrangements (e.g., Article 26(2)(d), which allows a data processor to enlist a subprocessor only with the prior permission of the data controller). Non-EU-based data controllers processing the data of EU citizens related to the offering of goods or services to them or to the monitoring of their behavior are obligated to appoint a representative established in an EU member state (Article 25), with some important exceptions as stated in Article 25(2) (such as when the controller is established in a country that has been found "adequate," the controller has fewer than 250 employees, or when the controller "only occasionally" offers goods or services to individuals in the EU). The representative is subject to substantial liability risks, since it is liable for penalties that can be levied against the controller (Article 78(2)).

The responsibilities of data processors as set forth in Article 26 are much more extensive than those contained in Article 17 of Directive 95/46, and will likely require amendment of contracts between data controllers and data processors (such as IT service providers and hosting companies). Data processors that exceed the data processing instructions given them by data controllers will be subject to all the obligations of controllers contained in Article 24 (Article 26(4)). Data controllers and processors, with some exceptions, also are responsible for keeping detailed documentation of all data processing operations, which must be produced upon request to DPAs (Article 28), though a late addition to the text exempts companies with fewer than 250 employees from this requirement (Article 28(4)). Article

[42] *See* the decision of the European Court of Justice in Joined Cases C-92/09 and C-93/09 *Volker und Markus Schecke* [2010] ECR I-0000, at para. 48.

[43] Explanatory memorandum, at 7.

[44] *See, e.g.*, Case C-275/06 *Promusicae* [2008] ECR I-271.

[45] *See* Recital 59.

29 requires controllers, processors, and the representatives of controllers to cooperate with DPAs.

The Proposed Regulation contains a number of important provisions concerning data security. Article 30 imposes wide-ranging data security obligations on both data controllers and data processors, the details of which are to be specified by the Commission. A general data breach notification requirement applicable horizontally to all types of data controllers[46] is also introduced, and notification of a breach is to be given by a data controller to both its lead DPA (Article 31) and the data subjects concerned (Article 32). Data processors are to notify the controller "immediately" after establishing that a breach has occurred (Article 31(2)). Notification is to be given by the controller to its lead DPA "without undue delay and, where feasible, not later than 24 hours after having become aware of it" (Articles 31(1)). The Commission impact assessment suggests that the requirement to notify should begin to apply at "the moment when the data controller records in its files that an event that triggered a first investigation has been identified as a personal data breach."[47] The 24-hour requirement was softened by addition of the words "where feasible" following the interservice consultation, and by a provision implying that notice within 24 hours need not be given when the data controller provides a "reasoned justification to the DPA as to why this time period could not be upheld" (Article 31(1));[48] thus, there are likely to be few cases in which notice must actually be given within 24 hours. This is a change for the better, as the 24-hour requirement is both inadvisable from a policy point of view and impossible to comply with in practice. Excessive notification of data security breaches has become a serious problem in other jurisdictions such as the United States that have long had security breach notification requirements,[49] and the 24-hour requirement only creates incentives for companies to over-notify, rather than to take the time to assess the situation in a thoughtful way and work with regulators to minimize the damage.[50] Data controllers also must notify affected data subjects of a breach, but only "when the personal data breach is likely to adversely affect the protection of the personal data or privacy of the data subject" (Article 32(1)). Notification to the data subject is to be made after notification to the DPA, and then "without undue delay" (Article 32(1)). Notification to the data subject is not required if the controller had implemented "appropriate technological protection measures" prior to the data breach (Article 32(3)); this will provide a powerful incentive for companies to improve their data security procedures and technologies.

Data protection impact assessments are to be carried out by data controllers and data processors in certain circumstances, some of which are clear (e.g., when processing biometric data, Article 33(2)(d)), but others of which are vague (e.g., when data processing operations "are likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes," Article 33(1)). However, during the interservice consultation a Recital was added (Recital 71) indicating that the requirement to conduct them should apply in particular "to newly established large scale filing systems, which aim at processing a considerable amount of personal data at regional, national or supranational level and which could affect a large number of data subjects"; this would presumably exclude most small and medium-sized enterprises (SMEs). In addition, provisions that would have required data protection impact assessments in most routine situations under which employee data are processed were deleted during the interservice process. The Commission estimates that such impact assessments can range in cost from €14,000 (approximately $18,400) for a small-scale one, to €34,500 (approximately $45,344) for a medium-scale one, and then to €149,000 (approximately $195,834) for a large-scale one.[51] In certain cases, multiple data controllers engaged in a common project may conduct a single impact assessment covering the entire project (Recital 72), which should reduce the burden. The Commission is empowered to specify the details of such assessments, which will likely reflect work already done at the European and member state level, such as by the Commission's radio-frequency identification Recommendation[52] and the "Privacy Impact Assessment Guideline" adopted in 2011 by the German Federal Office for Information Security (BSI).[53] Prior authorization of data processing by the DPA, or consultation with it, is required in some cases, as provided in Article 34. Significantly, a data processor may now under some circumstances consult the DPA on the data controller's behalf with regard to clarification of certain questions (Article 34(2)).

Data protection officers (DPOs) have long been required in some member states, but are almost totally unknown in others. The Proposed Regulation would make DPOs mandatory for all public authorities, and for all companies with more than 250 permanent employees (Article 35(1)). Articles 35–37 regulate in detail the designation, position, and tasks of DPOs, including requirements that they must exercise their duties in complete independence (Article 36(2)), and must be employed for at least two years (Article 35(7)). These provisions will create a new industry in the EU for the appointment, education, and training of DPOs.

[46] Article 4 of the e-Privacy Directive already includes a breach notification requirement that applies to providers of publicly available telecommunications services.

[47] Impact assessment, *supra* note 6, at Annex 5 at 84.

[48] *See also* Recital 67, stating that "[t]he need to implement appropriate measures against continuing or similar data breaches may justify a longer delay."

[49] *See* Fred C. Cate, The Centre for Information Policy Leadership, *Information Security Breaches: Looking Back and Thinking Ahead*, (2008), http://www.hunton.com/files/tbl_s47Details/FileUpload265/2308/Information_Security_Breaches_Cate.pdf.

[50] The Commission impact assessment seems to recognize this point, and states "A 'quick and dirty' notification rushed out to meet a deadline, which then requires updates and corrections will cause more insecurity concern and loss of confidence of data subjects than it provides benefits to users." Impact assessment, *supra* note 6, at Annex 5 at 84.

[51] Impact assessment*supra* note 6, at 79.

[52] Commission Recommendation of 12.5.2009 on the implementation of privacy and data protection principles in applications supported by radio-frequency identification, C(2009) 3200 final, http://ec.europa.eu/information_society/policy/rfid/documents/recommendationonrfid2009.pdf.

[53] *See* Bundesamt für Sicherheit in der Informationstechnik, *Privacy Impact Assessment Guideline* (2011), http://op.bna.com/pl.nsf/r?Open=kjon-8r5ts7.

PVLR ISSN 1538-3423

While the strengthening of the position of DPOs is a positive development, the provisions do raise certain questions. The threshold of 250 permanent employees means that in some member states (such as Austria, where there are few companies with this number of employees) most companies would be exempt from the requirement, while in others (such as Germany, which already has a requirement that most companies with over 10 employees must have a DPO) many companies that now have them would no longer be required to do so. The threshold of 250 employees was derived from the Commission definition of SMEs,[54] in order to exclude them, but it seems that many SMEs may still have to appoint a DPO, since the duty exists even for companies with fewer than 250 employees if their core activities "consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects" (Article 35(1)(c)). The Commission's impact assessment gives "head-hunters engaged in profiling activities" as an example of a company engaged in such systematic monitoring.[55] If the requirement to have a DPO is indeed to cover such activities that seem routine and can even benefit the individuals being profiled, then in fact many SMEs may have to appoint one.

Based on Article 35(2), it seems that a company with its headquarters in one member state and subsidiaries in others could appoint a single DPO based at the headquarters with functional responsibility over the subsidiaries as well. Thus, it will not be legally required to have a separate DPO physically based in each subsidiary, even if it may sometimes be practically advisable.

The Proposed Regulation also foresees the drafting of codes of conduct covering various data protection sectors, and allows them to be submitted to DPAs, which may give an opinion as to whether they are "in compliance with this Regulation" (Article 38(2)), and to the Commission, which may adopt implementing acts determining that codes "have general validity" (Article 38(4)). Presumably such determinations by a DPA or the Commission would mean that compliance with a code of conduct would also satisfy the legal requirements of the Proposed Regulation, but this should be made more explicit in the text. Finally, the establishment of "data protection certification mechanisms and of data protection seals and marks" also is encouraged, and the Commission may recognize them (Article 39), but again, the legal effect of such recognition should be clarified.

Chapter V: Data Transfer of Personal Data to Third Countries or International Organisations

General Principles—Adequacy Decisions—Appropriate Safeguards—Binding Corporate Rules—Derogations—International Cooperation

No topic addressed in the Proposed Regulation has received more attention than the transfer of personal data outside of the EU. Individuals, companies, DPAs, and governments all have been dissatisfied with the existing rules for various reasons, and reform of the legal framework for transborder data flows was one of the biggest challenges faced by the Commission. The proposed new rules make some valuable improvements to the current situation, but also raise many questions.

Article 40 abandons the presumption under Directive 95/46 that personal data may not be transferred absent an "adequate level of protection" in the recipient country, and instead sets forth general principles that must be fulfilled when data are transferred outside the EU. There are three categories of mechanisms that may legalize international data transfers, namely a Commission adequacy decision under Article 41; the use of "appropriate safeguards" under Article 42 (which include binding corporate rules under Article 43); or the application of a derogation under Article 44.

Article 41 expands the scope of Commission adequacy decisions somewhat, by explicitly providing that they may cover not only an entire country, but also a territory within a third country, a processing sector, or an international organization (Articles 41(1) and (3)). The fact that adequacy decisions may no longer be subject to any kind of authorization will reduce the administrative burden for data controllers in some member states that currently require them. The Proposed Regulation also gives the Commission increased power to decide that a territory, processing sector, or international organization does not provide adequate protection, and to enforce such decisions by prohibiting data transfers to it (Articles 41(5)–(6)). Unfortunately, the Proposed Regulation does not discuss at all the logistics of how adequacy decisions are to be issued, a process which is in urgent need of reform given the lengthy and convoluted procedures now in place. Article 41(2)(c), which provides that "the international commitments" a third country or international organization has entered into are to be assessed by the Commission in the process of deciding whether adequate protection exists, may increase the importance of Council of Europe Convention 108[56] by facilitating the approval of adequacy decisions for countries that have ratified it.

International data transfers also are possible if "appropriate safeguards" are in place (Article 42(2)), meaning one of the following mechanisms: binding corporate rules (BCRs); "standard data protection clauses" approved by the Commission (the counterpart of the present "standard contractual clauses"); standard data protection clauses adopted by a DPA in accordance with the consistency mechanism; "ad hoc" contractual clauses authorized by a DPA; or other appropriate safeguards "not provided for in a legally binding instrument." Of these, transfers based on ad hoc contractual clauses and those using other appropriate safeguards not provided for in a legally binding instrument require further authorization by the DPA (Article 34(1)). The fact that DPAs may no longer require authorization of transfers using the EU standard contractual clauses will be a great boon to data controllers. It is not clear what is meant by "other appropriate safeguards not provided for in a legally binding instrument" (Article 42(5)), but presumably this could include measures such as a code of best practices for a cloud computing service that was not contained in a contract or other legally-binding instrument, and which would then have to receive approval of the DPA. The Commission may also declare generally valid standard contractual clauses that have been adopted by DPAs (Article 42(2)(c)).

[54] *See* Recital 11.

[55] Impact assessment *supra* note 6, at 69.

[56] 28 January 1981, ETS 108.

Articles 41(8) and 42(5), together with Recital 134, confirm that despite the repeal of Directive 95/46, Commission decisions (such as adequacy decisions and those approving the standard contractual clauses) and those of DPAs remain in force; this language was not in the interservice version. Thus, data transfers under adequacy mechanisms that have already been approved (such as the U.S. Safe Harbor system), standard contractual clauses, and data transfer arrangements approved by DPAs can continue (though it is likely that the Commission may eventually merge the various sets of standard contractual clauses). However, the Proposed Regulation does raise some important questions about the functioning of certain adequacy decisions. For example, Article 40 seems to suggest that the conditions for data processing contained in the Proposed Regulation, and in particular those governing international data transfers, must also be applied to "onward transfers" of personal data that are sent to a third country and then subject to further transfers. Some Commission adequacy decisions (such as the safe harbor) already contain rules for conducting onward transfers, and it is not clear how such rules are to interact with the rules of the Proposed Regulation. The fact that the requirements for collecting and processing data in the EU will become much stricter under the Proposed Regulation also means that the threshold for transferring data outside the EU will effectively be raised (i.e., since no data may be transferred unless they were legally collected and processed in the first place, as provided in Article 40).

Explicit legal recognition of BCRs is to be welcomed, so that any remaining legal barriers to their use under member state law will be removed (Article 43). Use of BCRs is limited to companies in "the same corporate group of undertakings" (Recital 85). The Proposed Regulation also explicitly recognizes the use of BCRs for data processors, thus responding to a call that business has long made. The requirements for BCRs contained in Article 43 are generally similar to those that have been set forth already by the Article 29 Working Party. One difference concerns the liability rules. At present, the Working Party requires that the BCRs contain a duty for the EU headquarters of the company, or a delegated subsidiary in the EU, to assume liability for violations.[57] By contrast, the Proposed Regulation does not expressly require that the EU headquarters or a delegated subsidiary assume liability, but refers to acceptance of liability by a "controller or processor established on the territory of a Member State" (Article 43(2)(f)), which gives companies more flexibility in structuring their liability schemes. BCRs are to be approved by the DPAs using the consistency mechanism (Article 43(1)). The Commission also retains important powers to adopt delegated and implementing acts with regard to the format, procedures, and requirements for approval of BCRs (Article 43(3)–(4)). It is unfortunate that the provisions concerning BCRs fail to propose any way to lessen the burden on SMEs of complying with the data transfer restrictions.

The use of so-called "derogations" to transfer personal data is possible under Article 44, though their scope has been changed somewhat in comparison with Article 26 of Directive 95/46. In particular, new restrictions on the use of consent to transfer personal data are introduced (Article 44(1)(a)). One revolutionary change is introduced in Article 44(1)(h), which provides that "a data transfer may, under limited circumstances, be justified on a legitimate interest of the controller or processor, but only after having assessed and documented the circumstances of that transfer operation."[58] This new provision, which would require that data transfers be notified to the DPAs but not approved by them (Article 44(6)), seems to come close to the U.K. system of allowing self-assessment for international data transfers, though the fact that it cannot be used when the transfers can be described as "frequent or massive" (Article 44(1)(h)) would seem to rule it out in scenarios such as cloud computing. It is likely to prove controversial during the legislative process.

A provision in the interservice version that would have prohibited the transfer of personal data based on orders or requests from non-EU courts, tribunals, administrative authorities, and other governmental entities, unless mutual legal assistance treaties or procedures under international agreements were followed, or unless the relevant DPA had approved the transfer, was obviously targeted at requirements under U.S. law for the disclosure of data, in particular based on law enforcement requirements or e-discovery requests. However, this provision was unexpectedly deleted in the final version of the Proposed Regulation. Nevertheless, the Commission has stated publicly that the final sentence of Recital 90[59] may lead it to adopt restrictions on transfers compelled by foreign courts or governmental authorities.

Chapter VI: Independent Supervisory Authorities

Supervisory authorities—Independence—Membership and establishment of DPAs—Professional secrecy—Competence—Duties—Powers

The Proposed Regulation contains enhanced protections for the independence of the DPAs (Article 47), and provisions designed to ensure their effective functioning, which is important following the decision of the European Court of Justice in the case *Commission v Germany*,[60] in which the Court set high standards for DPA independence. The Proposed Regulation would reduce the powers of local DPAs in federal countries such as Germany, by requiring that a member states with multiple DPAs designate a single one for participation in the European Data Protection Board, and that the member state set out a single contact point to ensure effective participation by all of them in the European consistency mechanism (Recital 93; see below regarding the Board and the consistency mechanism), thus effectively preventing local DPAs from undercutting a harmonized EU data protection framework. The DPAs had been hoping that specific standards for funding of their operations would be included, but the Proposed Regulation adopts a vague requirement that each member state shall ensure that a DPA is provided with "adequate human, technical and financial resources, pre-

[57] Article 29 Working Party, "Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules" (WP 153, June 24, 2008), at 4.

[58] Explanatory memorandum, at 12.

[59] Reading with regard to Article 44(1)(d) that "The conditions under which an important ground of public interest exists should be further specified by the Commission in a delegated act."

[60] Case C-518/07 [2010] ECR I-01885.

PVLR ISSN 1538-3423

mises and infrastructure necessary for the effective performance of its duties and powers" (Article 47(5)), without specifying a formula for determining the adequacy of such support. The duties and powers of DPAs also are harmonized at a high level (Articles 52 and 53), so that many DPAs will have greater enforcement powers than they currently do.

Article 51 confirms that each DPA has jurisdiction on the territory of its own member state. Of great benefit to companies is the fact that if a data controller or data processor has establishments in multiple member states, the DPA of the member state of the company's main establishment is competent to supervise the data processing activities of the company in all member states (Article 51(2)). This rules establishes a "lead DPA" for companies with operations around the EU, so they can deal with a single DPA rather than with up to 27; the DPAs of the various member states where the company has operations are supposed to work together under the so-called mutual assistance and cooperation procedures under Articles 55–56 (discussed below) to ensure effective supervision. The details of what should be considered a data controller's "main establishment" are specified in Recital 27, which states that this should be the place of the company's "central administration," irrespective of whether the processing of personal data is actually carried out at that location. However, the Recital seems contradictory, as it also states that the determination of the main establishment should imply "the effective and real exercise of management activities determining the main decisions as to the purposes, conditions and means of processing through stable arrangements." In fact, there are many companies with decentralized corporate structures where the central administration and the place where management decisions about data processing are made may differ. It is also not clear how determination of the place of main establishment is to be made in practice, i.e., whether the company should make it, or whether a DPA will decide it, and how disputes in this regard are to be resolved. For data processors, the main establishment is its place of central administration in the EU (Recital 27). These rules will mean that, for instance, a smaller and less-resourced DPA in a member state where the company has its main establishment may become competent to supervise the company's activities all over the EU, which could place great pressure on its capacities and cooperation with other DPAs.

Individuals may bring suit against a controller or processor either before the courts of the member state where the controller or processor has an establishment (i.e., not just before those of its main establishment), or before those of the individual's habitual residence (except in the case of suits against public authorities under Article 75(2)).

Chapter VII: Cooperation and Consistency

Mutual assistance—joint enforcement—consistency mechanism—implementing acts—enforcement—European Data Protection Board

The harmonization of data protection law can only be achieved if the DPAs cooperate much more closely than has so far been the case, and if data protection rights can be enforced seamlessly across the entire EU. The Proposed Regulation contains several provisions designed to realize these objectives, including a duty for DPAs to take action on a request of another DPA within one month (Article 55(2)), and a provision empowering DPAs to conduct joint enforcement actions (Article 56). It is also provided that when, in certain circumstances, a DPA does not act within one month of being requested to by other DPAs, those other DPAs may take provisional enforcement or compliance actions in the member state of the first DPA (Articles 55(8) and 56(5)); this may cause a clash with constitutional law in some member states, since it affects basic principles of national sovereignty.

Of particular importance is the creation of a "consistency mechanism," which is designed to ensure that the DPAs take a more consistent view of data protection questions of common interest. In a highly-complex procedure too detailed to go into here, a DPA is supposed to communicate certain enforcement and compliance measures it intends to take in advance to the Commission and the European Data Protection Board (the successor to the Article 29 Working Party). The Board is then supposed to vote by a simple majority on the measure, and the DPA is to "take account" of the opinion of the Board, and communicate to it within two weeks whether it will take the measure or not (Article 58). The Commission is also supposed to adopt an opinion in relation to such measures, of which the DPAs are to take the "utmost account" (Article 59). The Commission has gained substantial powers to force the DPAs to take a more harmonized approach, since it may request that any matter be dealt with via the consistency mechanism (Article 58(4)), and may also adopt a reasoned decision requiring a DPA to suspend the adoption of a measure when it has "serious doubts as to whether the draft measure would ensure the correct application of the Regulation or would otherwise result in its inconsistent application" (Article 60(1)). It is questionable whether these powers are consistent with the independence of the DPAs, and they are likely to be politically controversial. DPA decisions and measures are made enforceable in all member states, except when the DPA did not convey them to the Commission and the Board under the consistency mechanism (Article 63(2)).

As stated earlier, the Article 29 Working Party is renamed "European Data Protection Board," and its functioning is set out in more detail than in Directive 95/46. The secretariat of the Board is moved from the Commission to the European Data Protection Supervisor (EDPS) (Article 71), though the Commission remains an observer (Article 64(4)). This would seem to free up resources in the Commission for other tasks, such as adopting delegated and implementing acts, and will increase the power of the EDPS, which can be seen as one of the "winners" of the Proposed Regulation. The Board is to be independent (Article 65), and its tasks (Article 66) and decision-making procedures (to be taken by a simple majority of members, Article 68(1)) are also set forth.

Chapter VIII: Remedies, Liability and Sanctions

Complaints to DPAs—judicial remedies against DPAs—judicial remedies against controllers and processors—court proceedings—compensation and liability—penalties—administrative sanctions

There have long been complaints that the DPAs lack uniform enforcement powers, and that the available mechanisms to sanction data protection violations were insufficient, which have been addressed in the Pro-

posed Regulation. Article 73(1) provides that an individual in any member state can lodge a complaint with any DPA, not just the one where they reside. The draft also gives organizations and associations the right to bring claims before the DPAs, both on behalf of individuals (Article 73(2)) and on their own behalf (Article 73(3)). These types of collective actions are already used in some member states.[61] However, these changes stop short of adopting the U.S. system of "class actions," since they do not foresee the adoption of other changes to member state law that would be necessary to adopt such a system (such as a change to the "loser pays" rule for litigation costs). The Proposed Regulation would provide both natural and legal persons with the right to launch a judicial action against DPAs (Article 74(1)), including the possibility for an individual to request a DPA to bring suit against another DPA (Article 74(4)). Member states are obliged to enforce final court decisions against DPAs (Article 74(5)) or against a data controller or processor (Article 75(4)) in any member state, just as they are with regard to decisions of DPAs (Article 63(1)) (though with regard to DPA decisions, it is not clear if what is meant is that they are enforceable in court, or by other DPAs, or both).

Highly significant is the new regime for penalties and administrative fines, which are, for the first time in the history of data protection law, of such a magnitude that they will get attention from companies' CEOs and general counsel. Indeed, one of the purposes of the Proposed Regulation seems to be to elevate the significance of data protection so that it is on a par with other corporate compliance topics such as competition law, antibribery, and money laundering requirements. Besides the size of the penalties, all controllers and processors involved in the data processing are jointly and severally liable for the entire amount of any damage suffered, unless they can prove that they are not responsible for the event giving rise to the damage (Article 77(2–3)). However, the drafters should have included here a reference to Article 24, so that joint data controllers could apportion their liability in advance by means of a written agreement. The representative of a non EU-based data controller is also liable for any penalties assessed against the controller (Article 78(2)).

Under Directive 95/46, the amount of administrative sanctions was left to implementation by the member states,[62] with the result that they varied widely. The sanctions that may be imposed on companies under the Proposed Regulation are hugely increased over what was previously possible. They are to be imposed mandatorily for any intentional or negligent violation of certain provisions of the Proposed Regulation, and are divided into three categories, ranging from up to 0.5 percent, 1 percent, or 2 percent of a company's annual worldwide turnover (i.e., its worldwide revenues) respectively (Articles 79(4)–(6)). To give an example of the potential maximum amount of such a fine, Google's annual revenues in 2010 were approximately $29 billion,[63] 2 percent of which would be approximately $580 million (approximately €439 million). The Commission has suggested publicly that there is an exemption for a company's first violation, but in fact the text only gives DPAs the power to abstain from a fine in cases where the violation is committed by a natural person processing data without a commercial interest, or by an organization with fewer than 250 employees that processes personal data "only as an activity ancillary to its main activities" (Article 79(3)). So in the vast majority of cases such exemption will not apply.

The provisions on fines and penalties give rise to some questions. For example, the wording in Article 79(1) that sanctions may be imposed by "each supervisory authority" suggests that in theory a company could be sanctioned separately by 27 different DPAs for the same violation if it occurred within each jurisdiction, which stands in contradiction to the fact that supervision of a company is limited to the DPA of the company's main establishment (Article 51(2)). While this is not explicitly stated, the imposition of fines presumably should be subject to the consistency mechanism, since it constitutes "a measure intended to produce legal effect" under Article 58(2).[64] Some of the grounds for which penalties can be imposed seem overly burdensome or unclear. A couple of examples include situations when joint data controllers do not sufficiently "determine the respective responsibilities with co-controllers pursuant to Article 24" under Article 79(5)(e), which would require companies to renegotiate many or all of their contracts with outside vendors or face penalties; and the fact that a sanction may be imposed for not "timely or completely notifying" a data breach to the supervisory authority or to data subjects pursuant to Article 79(6)(h), which seems unreasonable given that what constitutes "complete notification" is likely to be a matter of opinion. The text of Article 79 also obliges the DPAs to impose administrative penalties ("*shall* impose a fine" (*emphasis added*)), whereas it would have been more appropriate to allow them to do so ("*may* impose a fine"). It can also be questioned why the administrative sanctions under the Proposed Regulation are so Draconian and detailed, while those for violations by public authorities of data processing requirements in the criminal justice sector as set out in the Proposed Directive are so vague and are left entirely up to the member states.[65]

Chapter IX: Provisions Relating to Specific Data Processing Situations

Freedom of Expression—Processing for Health Purposes—Employment Data Processing—Historical, Statistical and Scientific Research—Secrecy—Existing Rules of Churches and Religious Associations

The Proposed Regulation contains articles dealing with a number of specific data processing situations. Article 80 requires member states to provide exemptions or derogations for the processing of personal data for journalistic purposes or for artistic and literary expression, and is an elaboration of Article 9 of Directive 95/46. The definition of "journalistic activities" as explained in Recital 121 reflects the broad interpretation of that term by the European Court of Justice in the

[61] For example, in Austria (§ 29 *Konsumentenschutzgesetz*) and Germany (§ 3 *Unterlassungsklagegesetz*).

[62] Directive 95/46, Article 24.

[63] *See* Google Investor Relations, 2011 Financial Tables, http://investor.google.com/financial/tables.html.

[64] *See also* Recital 120, stating that "the consistency mechanism may also be used to cover divergences in the application of administrative sanctions."

[65] *See* Proposed Directive, Article 55.

PVLR ISSN 1538-3423

case *Satamedia*,[66] and would include activities carried out by individuals without making a profit (e.g., by internet bloggers). Articles 81 and 82 encourage member states to enact legislation covering the subjects of data processing for health purposes and data processing in the employment context respectively, which will likely lead to more legislation at the national level in these areas. While the Commission is empowered to adopt delegated acts in both fields, it is to be feared that an increase in national legislation may lead to a lack of harmonization. Directive 95/46 has been criticized for inhibiting historical, statistical, and scientific research,[67] and Article 83 attempts to deal with this by providing more detailed rules for such processing. Article 84 contains enhanced obligations of secrecy for investigations by DPAs of data controllers or processors who are themselves subject to obligations of professional secrecy (such as doctors and lawyers). An article added during the interservice procedure provides that data processing rules used by churches and religious associations may continue to be used, provided they are brought into line with the Proposed Regulation (Article 85).

Chapter X: Delegated Acts and Implementing Acts

Exercise of Delegation—Committee Procedure

One of the most striking elements of the Proposed Regulation is the number of instances in which the Commission has granted itself the power to adopt so-called "delegated acts" or "implementing acts," both of which may take the form of a regulation, a directive, or a decision,[68] though they are adopted under different procedures than are normal legislative instruments under the co-decision procedure. The scope, functionality, and effects of these acts have been the subject of controversy in the legal literature,[69] and a full analysis of them would exceed the scope of this article. Suffice it to say that delegated acts are designed to supplement or amend non-essential elements of EU legislative acts,[70] while implementing acts are designed simply to implement them.[71] The distinction is important, since the procedures for review and scrutiny of these two types of acts differ substantially: the European Parliament and the Council exercise extensive scrutiny over delegated acts, including the right to reject the Commission's proposed measure in certain cases,[72] whereas the adoption of implementing acts is subject to a complex series of committee procedures laid down in a separate EU regulation[73] and is largely under the control of the Commission, with input from the Council but without any from the European Parliament.[74] In most cases implementing acts, the legal basis for which is specified in Article 62, are to be adopted under the so-called "examination procedure," whereas in a few cases of particular urgency (such as under Article 41(5)) an expedited procedure may be used. In adopting implementing acts, the Commission is to be assisted by a committee comprised of member state representatives (Article 87), which will in effect play the role that the Article 31 Committee plays under Directive 95/46. The legality of both delegated and implementing acts can be reviewed by the European Court of Justice.[75]

In total there are 26 instances[76] in the Proposed Regulation where the Commission grants itself the power to adopt delegated acts, and 19 instances[77] where it may adopt implementing acts, which is a relatively high number (note that there are some mistakes in the numbering of articles in Article 86).[78] In fact, there is scarcely any topic of importance that will not be substantially affected based on a delegated act or an implementing act. Article 62(1)(a) also seems to give the Commission the power to issue a virtually unlimited number of additional implementing acts, since it may do so in order to decide "on the correct application of this Regulation in accordance with its objectives and requirements in relation to matters communicated by supervisory authorities pursuant to Article 58 or 61, concerning a matter in relation to which a reasoned decision has been adopted pursuant to Article 60(1), or concerning a matter in relation to which a supervisory authority does not submit a draft measure and that supervisory authority has indicated that it does not intend to follow the opinion of the Commission adopted pursuant to Article 59." The Proposed Regulation can thus be seen as a kind of torso that is to be fleshed out by further measures to be taken by the Commission. The large numbers of both types of acts will result in a substantial shifting of power regarding data protection policymaking from the EU member states and the DPAs to the Commission. This shifting of power will result in substantial political opposition; the willingness of the Commission to make such acts revocable at any time by the European Parliament and the Council (Article 86(3)), or to allow them to come into effect only if the Parliament and the Council have not objected to them (Article 86(5))—possibilities that are allowed but not mandated under Article 290(2) of the Treaty on the Functioning of the European Union—demonstrates that the Commission is trying to forestall objections to its powers by other EU institutions and the member states.

Legal commentators have predicted that it will often be difficult to determine whether a particular measure should be adopted based on a delegated act or an implementing act,[79] and in fact there are several examples in the Proposed Regulation where the rationale for designating an act as one type or another seems unclear. To give one example, the "particular circumstances in which a controller and a processor" are required to pro-

[66] Case C 73/07 [2008] ECR I-09831, para. 61.

[67] *See* David Erdos, *Stuck in the Thicket? Social Research under the First Data Protection Principle*, 19(2) International Journal of Law and Information Technology 133 (2010).

[68] Paul Craig, *The Lisbon Treaty* 254–55 (Oxford Univ. Press 2010).

[69] *See, e.g., id.*, at 260–82.

[70] *See* Article 290 TFEU.

[71] *Id.* at Article 291.

[72] *Id.* at Article 290(2).

[73] Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by Member States of the Commission's exercise of implementing powers [2011] OJ L55/13.

[74] Craig, *supra* note 68, at 275.

[75] *See* Article 263 TFEU (n 16), referring to review by the ECJ of "acts . . . of the Commission."

[76] *See* the list in Article 86.

[77] By the author's count. *See* the description in Recital 130.

[78] For example, references to Article 20(6) should read 20(5) (there is no Article 20(6)), and references to Article 79(6) should read 79(7) (there is no reference to delegated acts in Article 79(6)).

[79] *See* Craig, *supra* note 68, at 277–79.

vide notification of a personal data breach are to be determined by a delegated act (Article 32(5) of the Proposed Regulation), but the "procedures applicable to the notification requirement" are to be determined by an implementing act (Article 32(6)). In fact, these two matters seem so closely related that they could be dealt with as part of a single act and by either of the two categories of acts.

Another issue concerns the resources necessary for the Commission to adopt so many acts, and the time frame for their adoption. Many of the issues about which acts are to be adopted are complex and subject to disagreement even among experts (an example is determining the lawfulness of data processing based on balancing the legitimate interests of the data controller against the interests or fundamental rights of data subjects, conditions that are to be determined by a delegated act of the Commission (Article 6(5)). In addition, since important details of many provisions will only become clear once the relevant delegated and implementing acts have been adopted, it is essential that the Commission be able to do so soon after the Regulation is enacted. However, the complexity of the issues involved, together with political forces, likely will lead to a delay in adoption of many of them, which could leave data controllers and processors with little guidance as to how to implement the Regulation in practice. This assumption is supported by the "Legislative Financial Statement" attached to the Proposed Regulation, which estimates that "up to three implementing measures may be handled per year, while the process may take up to 24 months,"[80] meaning that it would take 15 years for all 45 delegated and implementing acts to be enacted. It would seem fair and proportionate to delay the imposition of fines for a violation, the details of which are to be specified in a delegated or implementing act, until that act has been adopted, otherwise parties will not have enough information about how to comply with the law to avoid being sanctioned.

Chapter XI: Final Provisions

Repeal of Directive 95/46—e-Privacy Directive—Evaluation—Entry into Force and Application

Under Article 88, Directive 95/46 is repealed and references to it are to be construed as references to the Proposed Regulation. The Proposed Regulation is directly applicable in the member states (recital following Article 91), so that it does not need to be implemented into national law. The relationship between the Proposed Regulation and the e-Privacy Directive[81] is clarified by a provision incorporated following the interservice consultation, which stated in effect that the e-Privacy Directive (as the more specialized instrument) takes precedence over the Proposed Regulation on points that both of them deal with, i.e., the Proposed Regulation does not impose extra obligations in areas already covered in the e-Privacy Directive (Article 89). For reasons of consistency and efficiency, it would have been preferable to incorporate the e-Privacy Directive into the Proposed Regulation as well, particularly since many of its provisions seem to be targeted at the electronic communications sector that is the focus of the e-Privacy Directive. The e-Privacy Directive is to be amended in light of the Proposed Regulation (Recital 135), but it is unlikely that this will occur before the Proposed Regulation is adopted.

The Commission is to submit evaluation reports on the Proposed Regulation to the European Parliament and the Council at regular intervals, initially no later than four years after its entry into force (Article 90); the national DPAs (Article 54) and the European Data Protection Board (Article 67) also are supposed to publish annual reports of their activities. It is to be regretted that the Proposed Regulation does not foresee the establishment of a permanent stakeholder group or expert advisory group to provide input to the Commission on how it is functioning in practice. It is to enter into force on the 20th day after its publication in the EU Official Journal, and shall apply as of two years from that date (Article 91). Thus, the Proposed Regulation will likely not come into force before 2015 at the earliest.

IV. Conclusions

The Proposed Regulation deserves to be considered a "Copernican revolution" in EU data protection law. It constitutes a bold attempt to make the legal framework more efficient and effective; increase protection of fundamental rights; and provide more legal certainty. Such a complete revision is justified, as it has been widely recognized that Directive 95/46 is out of date, and given the current political climate, the revision process now underway may be the best opportunity to update the framework for the foreseeable future.

Some of the reforms are highly welcome. For example, because the Proposed Regulation would be directly applicable, it would provide as near complete harmonization as is possible under EU law. It would also make companies with operations in multiple EU member states subject to the jurisdiction of a single DPA, based on their main place of establishment in the EU. Notifications to DPAs of data processing activities would be eliminated. The legal certainty of "adequacy" decisions and standard contractual clauses for transferring data outside the EU would be increased, and BCRs would be explicitly recognized. DPAs would be forced to cooperate, and the Commission would be empowered to issue EU-wide interpretations of important provisions. These are all highly significant improvements to the legal framework, and represent changes that business has been requesting for years.

It is much easier to criticize such an ambitious proposal than to draft one. Nevertheless, the Proposed Regulation also gives grounds for criticism. First of all, it sometimes loses sight of the need to adopt provisions that can actually be implemented in practice, and to be precise and meticulous in drafting. While the text emphasizes the need for data controllers to use understandable language,[82] it is equally important that legislation be written so that it can be easily used by nonlawyers and businesspeople unacquainted with data protection. In fact, the text abounds with legalistic jar-

[80] Proposed Regulation, Legislative Financial Statement, at 114.

[81] Directive (EC) 2002/58 of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector [2002] OJ L201/37, amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 [2009] OJ L337/11.

[82] *See* Article 11(2), requiring controllers to provide information and communications to data subjects "in an intelligible form, using clear and plain language . . . ."

PVLR ISSN 1538-3423

gon that many businesspeople will be able to make little sense of, for example, "The data subject shall have the right to obtain from the controller communication to each recipient to whom the data have been disclosed of any rectification or erasure carried out in compliance with Articles 14 and 15. . ." in Article 11. The text also contains several examples that seem merely illustrative and could better be included in the explanatory memorandum or in a recital; for example, the right to be forgotten is said to apply "especially in relation to personal data which are made available by the data subject while he or she was a child" (Article 17(1)), but it is unclear what the legal effect is of saying that the right applies "especially" to such data, or whether any special legal effect was intended at all.

The commendable reduction of bureaucracy in some areas is at least partially offset by the introduction of other procedural requirements (such as the need to keep extensive internal documentation of data processing). While a number of last-minute changes to the text were adopted to reduce the burden put on SMEs, it can be feared that they still will be burdened by extra costs. Despite its status as a regulation, the use of vague language is likely to lead to difficulties of interpretation, and may cause greater divergence in national approaches than the Commission thinks. Basic differences in legal systems and administrative cultures in member states may be one of the greatest risks to the Proposed Regulation, since these are not easily susceptible to harmonization from Brussels.

In addition, some of its specific innovations seem misguided. The "right to be forgotten" seems to be a version of the existing right to erasure which has been extended so far as to pose risks to other fundamental rights and to the use of the internet. The rules on profiling will prove difficult to understand and apply in practice. And while there is a need for more stringent enforcement of the law and more harmonized enforcement powers, the combination of ill-defined offenses and huge mandatory fines raises basic questions of fairness.

Another point of concern relates to the role of EU data protection law in the current global environment. The apparent assumption that the majority of international data transfers can be legalized by the use of BCRs and standard contractual clauses insufficiently takes into account the realities of massive international data transfers via phenomena such as cloud computing. It is also unfair that the requirements for transferring personal data internationally for criminal justice purposes under the Proposed Directive are much more lenient than are those under the Proposed Regulation.[83] The significant changes brought about by the Proposed Regulation may also make it more difficult to achieve interoperability between the EU legal framework and those in other regions. The Proposal also contains a whiff of protectionist language.[84]

While the Proposed Regulation would in general harmonize the law at a high level, some member states may raise legitimate questions as to the affect it would have on data protection in their own countries. For example, a member state such as Austria has only a very small number of companies with over 250 employees, and thus the vast majority of companies there will be exempt both from the duty to appoint a DPO and from the documentation requirements, while the duty to notify the DPA of data processing also would be eliminated. Since the requirement to appoint a DPO and to keep documentation of data processing would be introduced largely as a replacement for the notification requirement,[85] one might be legitimately concerned about how the fact that none of these three requirements would apply in a number of member states would affect the level of data protection in them. It also seems counterproductive to raise the threshold for appointment of a DPO so high in a country like Germany where their use has been a success.

Despite the above criticisms, the author's overall view of the Proposed Regulation is cautiously positive, as it constitutes an improvement on Directive 95/46, and demonstrates a commendable willingness to take on some of the "sacred cows" of data protection law that have outlived their usefulness. For the private sector, the final success of the Proposed Regulation will perhaps depend on three key factors, namely the effectiveness of the "lead DPA" concept; the operation of the consistency mechanism; and the ability of the Commission to issue delegated and implementing acts of high quality in a way that is timely and transparent and gives stakeholders an opportunity to provide input. If these three factors are realized, then it may work as designed to bring about a more harmonized level of data protection throughout the EU, and the benefits could be great for data controllers, individuals, and the EU economy. But if they are weakened during the EU legislative process, or if member states and DPAs undermine them, then many of the other positive changes foreseen in the text may lose much of their effect. Only time will tell if the final result is a revolution that brings about lasting improvements.

---

[83] *See* Proposed Directive, Article 35(1)(b), stating that a transfer of personal data to a recipient in a third country or to an international organization is permissible when "the controller or processor has assessed all the circumstance surrounding the transfer of personal data and concludes that appropriate safeguards exist with respect to the protection of personal data."

[84] *See* Impact assessment*supra* note 6, at 89, stating that the Proposal can lead to "long-term improvements for European businesses," and that "non-EU companies which do not have appropriate standards will be limited in their ability to operate within the EU . . . ."

[85] This is clearly stated on pages 10-11 of the explanatory memorandum.