Santa Clara High Technology Law Journal

Volume 28 | Issue 4 Article 3

9-10-2012

European Data Protection 2.0: New Compliance Requirements in Sight - What the Proposed EU Data Protection Regulation Means for U.S. Companies

Francoise Gilbert

EUROPEAN DATA PROTECTION 2.0: NEW COMPLIANCE REQUIREMENTS IN SIGHT—WHAT THE PROPOSED EU DATA PROTECTION REGULATION MEANS FOR U.S. COMPANIES

Francoise Gilbert[†, ††]

The proposed data protection package that the European Commission unveiled on January 25, 2012 provides a sneak preview of the plans for a comprehensive reform of the data protection rules in the European Union. The new data protection framework would be based on two documents: a Regulation,[1] which would address the general privacy issues, and a Directive,[2] which would address the

---

Francoise Gilbert, JD, CIPP/US, focuses her legal practice on information privacy and security, cloud computing, and data governance. In the past 12 months, she was voted one of the country's top legal advisors on privacy matters in an industry survey, and named "an attorney who matters" by Ethisphere. In addition, for several years, has been recognized by *Chambers* and *Best Lawyers* as a leading lawyer in the field of information privacy and security. Gilbert is the author and editor of the two-volume treatise *Global Privacy & Security Law* (Aspen Publishers / Wolters Kluwer Law and Business) (2012) (http://www.globalprivacybook.com), which analyzes the data protection laws of 65 countries on all continents. She is the managing attorney of the IT Law Group (http://www.itlawgroup.com) a niche law firm that focuses on information privacy and security and cloud computing, and serves as the general counsel of the Cloud Security Alliance. She writes a monthly column for TechTarget on cloud computing issues (http://searchcloudsecurity.techtarget.com/contributor/Francoise-Gilbert), and keeps a blog on domestic and international data privacy and security issues (http://www.francoisegilbert.com). She can be reached at (650) 804-1235 or fgilbert@itlawgroup.com.

†† Ms Gilbert would like to thank the entire team of editors and associates at the Santa Clara Computer and High Technology Law Journal for their hard work in the production and publication of this article. Special thanks to Darryl Ong, Senior Production Editor, and Teri Karobonik, Lead Production Editor for their outstanding and tireless work in the development and review of the footnotes, and verification of the sources for all assertions. Special thanks, as well, to Michael VanAuker, Editor-in-Chief and Chris Dombkowski, Managing Editor for their editing and review of the final drafts and their management of the team.

1. *Commission Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data (General Data Protection Regulation)*, COM (2012) 11 final (Jan. 25, 2012) [hereinafter *Proposed Regulation*], *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:EN:PDF.

2. *Commission Proposal for a Directive of the European Parliament and of the Council*

unique issues associated with criminal investigations. The proposed legislative texts are intended to redefine the legal framework for the protection of personal data throughout the European Economic Area.[3] The vision revealed in the documents published on January 25, 2012[4] is generally consistent with the plan of action that was presented in late 2010.[5] What is new, or was not clearly specified in 2010, is the shift to a single law that would be common to all of the Member States.[6]

The publication of the Proposed Regulation and Proposed Directive signals a very important shift in the way data protection will be handled in the future throughout the European Union. If the draft legislative texts are adopted in a form substantially similar to that which was presented on January 25, by 2015[7], the European Union Member States will be operating—for most types of activities—under a single data protection law that applies directly to all entities and

---

on the Protection of Individuals with Regard to the Processing of Personal Data by Competent Authorities for the Purposes of Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and the Free Movement of such Data, COM (2012) 10 final (Jan. 25, 2012) [hereinafter *Proposed Directive*], *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0010:FIN:EN:PDF.

3. For an in-depth analysis of the current data protection framework in effect in the European Union, see generally, FRANCOISE GILBERT, GLOBAL PRIVACY AND SECURITY LAW, (supp. #7 2012). In particular, see Chapter 3 "Genesis of Modern Information Privacy and Security Law," Chapter 4 "The Byzantine Process of European Data Protection Law Making," Chapter 5 "Introduction to the European Union Data Directives," Chapter 6 "1995 EU Data Protection Directive," Chapter 7 "2002 EU Directive on Privacy and Electronic Communications," Chapter 8 "2006 Data Retention Directive," and Chapter 9 "Transferring Personal Data out of the European Union and European Economic Area."

4. *Proposed Regulation*, *supra* note 1; *Proposed Directive*, *supra* note 2.

5. *See generally Communication from the Commission: A Comprehensive Approach on Personal Data Protection in the European Union*, COM (2010) 609 final (Nov. 4, 2010) [hereinafter *Communication 609*], *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0609:FIN:EN:PDF; *see also* GILBERT, *supra* note 3 (Chapter 5 "The European Union Data Directives").

6. *Communication from the Commission: Safeguarding Privacy in a Connected World: A European Data Protection Framework for the 21st Century*, at 8-9, COM (2012) 9 final (Jan. 25, 2012) [hereinafter *Safeguarding Privacy*], *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0009:FIN:EN:PDF. ("To enhance the Single Market dimension of data protection, the Commission proposes to: lay down data protection rules at EU level through a Regulation directly applicable in all Member States which will put an end to the cumulative and simultaneous application of different national data protection laws." (citations omitted)).

7. *See id.* at 2 n.2 (citing Conclusions (EC) No. EUCO 52/1/11 of 23 October 2011) ("See also the conclusions of the European Council of 23 October 2011, which stressed the "key role" of the Single Market "in delivering growth and employment," as well as the need to complete the Digital Single Market by 2015.").

individuals.[8] In many cases, companies will no longer have to suffer the fragmentation resulting from the significant discrepancies in the manner in which the 27 Member States interpreted and implemented the principles set forth in Directive 95/46/EC to create 27 different sets of national laws.[9]

A single set of rules on data protection, valid across the EU, would make it easier for companies to know and understand the rules. Unnecessary administrative burdens, such as notification requirements for companies,[10] would be abolished.[11] Instead, the proposed Regulation provides for increased responsibility and accountability for those processing personal data.[12] In the new regime, organizations would only have to deal with a single national data protection authority in the EU country where they have their main establishment.[13] Likewise, people would be able to refer to the

---

8. *See Safeguarding Privacy*, *supra* note 6; GILBERT, *supra* note 3, at 4-29 to 4-30 ("EU Regulations . . . are directly binding upon the Member States. As soon as they are passed, the EU Regulations become part of the national legal systems automatically . . . ."; "A directive is not incorporated "as is" in the law of a country. [A] Member State has to adapt its laws so that they meet the goals identified in the directive.").

9. Council Directive 95/46/EC, art. 4, 1995 O.J. (L 281) 31-50 (EC), *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:1995:281:0031:0050:EN:PDF; *Safeguarding Privacy*, *supra* note 6, at 7-8 ("Despite the current Directive's objective to ensure an equivalent level of data protection within the EU, there is still considerable divergence in the rules across Member States. Therefore, data controllers may have to deal with 27 different national laws and requirements. The result is a fragmented legal environment, which has created legal uncertainty and uneven protection for individuals. This has caused unnecessary costs and administrative burdens for businesses . . . . A Regulation will do away with the fragmentation of legal regimes across 27 Member States . . . .").

10. *See* Council Directive 95/46, arts. 18-21, 1995 O.J. (L 281) 43-44 (EC).

11. *Safeguarding Privacy*, *supra* note 6, at 8 ("To enhance the Single Market dimension of data protection, the Commission proposes to: . . . simplify the regulatory environment by drastically cutting red tape and doing away with formalities such as general notification requirements . . . .").

12. *Proposed Regulation*, *supra* note 1, at 27 ("Comprehensive responsibility and liability of the controller for any processing of personal data carried out by the controller or on the controller's behalf should be established. In particular, the controller should ensure and be obliged to demonstrate the compliance of each processing operation with this Regulation."). *See also id.* at 8-10 (Article 14 clarifies obligations of controllers as "building on Articles 10 and 11 of Directive 95/46/EC" and Article 26 clarifies obligations of processors "partly based on Article 17(2) of Directive 95/46/EC, and adding new elements, including that a processor who processes data beyond the controller's instructions is to be considered as a joint controller."). *See also id.* at 48-50 (text of Article 14). *See also id.* at 55-59 (text of Articles 22-28).

13. *Safeguarding Privacy*, *supra* note 6, at 8 ("To enhance the Single Market dimension of data protection, the Commission proposes to: . . . set up a 'one-stop-shop' system for data protection in the EU: data controllers in the EU will only have to deal with a single [Data Protection Authority (DPA)], namely the DPA of the Member State where the company's main establishment is located;"); *Proposed Regulation*, *supra* note 1, art. 51(2), at 77 ("Where the

data protection authority in their country, even when their data are processed by a company based outside the EU.[14]

The proposed reform would create more obligations for companies[15] and more rights for individuals,[16] while removing some of the administrative burdens that currently cost billions of Euros to companies.[17] However, numerous additional requirements would

---

processing of personal data takes place in the context of the activities of an establishment of a controller or a processor in the Union, and the controller or processor is established in more than one Member State, the supervisory authority of the main establishment of the controller or processor shall be competent for the supervision of the processing activities of the controller or the processor in all Member States, without prejudice to the provisions of Chapter VII of this Regulation.").

14. *See Proposed Regulation*, *supra* note 1, art. 73(1), at 89 ("[E]very data subject shall have the right to lodge a complaint with a supervisory authority in any Member State if they consider that the processing of personal data relating to them does not comply with this Regulation."); *id.* at 42 (defining a 'representative' as "any natural or legal person established in the Union who, explicitly designated by the controller, acts and may be addressed by any supervisory authority and other bodies in the Union instead of the controller, with regard to the obligations of the controller under this Regulation").

15. *See*, *e.g.*, *Proposed Regulation*, *supra* note 1, at 58-65 (imposing obligations on controllers and processors to maintain documentation of processing operations under their responsibility (Article 28), to implement appropriate measures for the security of processing (Article 30), to notify on personal data breaches (Article 31-32), to conduct data protection impact assessments prior to certain processing operations (Article 33), and to appoint a data protection officer); *Safeguarding Privacy*, *supra* note 6, at 6-7 (proposed rules will "[e]nhance the accountability of those processing data" by requiring designation of a Data Protection Officer in companies with more than 250 employees, mandating data protection safeguards be designed into procedures and systems and imposing the obligation to conduct data protection impact assessments).

16. *See*, *e.g.*, *Proposed Regulation*, *supra* note 1, at 50-53 (providing for the right of access for the data subject (Article 15), the right to rectification (Article 16), the right to be forgotten and to erasure (Article 17), the right to data portability (Article 18), and the right to object (Article 19)).

17. *Impact Assessment* accompanying *Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data (General Data Protection Regulation) and Directive of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data by Competent Authorities for the Purposes of Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and the Free Movement of such Data*, at 20, SEC(2012) 72 final, (Jan. 25, 2012) [hereinafter *Impact Assessment Report*], *available at*
http://ec.europa.eu/governance/impact/ia_carried_out/docs/ia_2012/sec_2012_0072_en.pdf.
("The administrative burden resulting from the fragmentation within the EU internal market is estimated at about € 2.9 billion per annum, accounting for about half of the overall administrative burden linked to the [95/46/EC] Directive (i.e. about € 5,3 billion)." (citations omitted)); *id.* at 73 ("The costs of current legal fragmentation for economic operators only in terms of administrative burden are estimated to amount to more than € 2.9 billion in total per annum. The expected net savings for economic operators would be around € 2.3 billion per annum, arising from the elimination of legal fragmentation and the simplification of notifications (basic registration).").

come instead. While the new data protection regime would reduce red tape, it would require entities to be more accountable,[18] to have in place written procedures and processes that they actually use,[19] and to be able to show that they do comply with the applicable legal requirements.[20] Entities would be responsible for conducting privacy impact assessments in some circumstances,[21] to comply with individual requests to exercise their "right to be forgotten,"[22] and to notify data protection authorities and individuals in the event of a breach of security.[23]

U.S. companies that do business in or with the European Economic Area should start preparing for this dramatic change in the data protection landscape. Some of the provisions will require the development of written policies and procedures, documentation, and applications as necessary to comply with the new rules. Security breaches will have to be disclosed,[24] and incident response plans will have to be created accordingly. The development of these new structures will require significant investment and resources. IT and IS departments in companies will need to obtain greater, more significant budgets in order to finance the staff, training, policies, procedures and technologies that will be needed to implement the new provisions.

---

18. *Safeguarding Privacy*, *supra* note 6, at 6-7 (proposed rules will "[e]nhance the accountability of those processing data" by requiring designation of a Data Protection Officer, ensuring data protection safeguards are designed into procedures and systems and imposing the obligation to conduct data protection impact assessments).

19. *Proposed Regulation*, *supra* note 1, art. 28, at 58-59 ("Each controller and processor and, if any, the controller's representative, shall maintain documentation of all processing operations under its responsibility" including "the description of the mechanisms referred to in Article 22(3)."); *id.*, art. 22(3), at 55 (requiring mechanisms to verify the effectiveness of policies adopted and measures implemented in compliance with the proposed regulation).

20. *Proposed Regulation*, *supra* note 1, art. 22(3), at 55 ("If proportionate, this verification shall be carried out by independent internal or external auditors.").

21. *Id.*, art. 33(1), at 62-63 ("Where processing operations present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes, the controller or the processor acting on the controller's behalf shall carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.").

22. *Id.*, art. 17, at 51-53 (Article 17: right to be forgotten and right to erasure).

23. *Id.*, arts. 31-32, at 60-62 (Article 31: notification of a personal data breach to the supervisory authority; Article 32: communication of a personal data breach to the data subject).

24. *Id.* (mandating disclosures to the supervisory authority within 24 hours for all personal data breaches, and if "likely to adversely affect the protection of the personal data or privacy of the data subject, . . . to the data subject without undue delay.").

1. THE FOUNDATION DOCUMENTS

The proposed data protection package contains two important legislative texts and an introductory document in the form of a Communication,[25] which provides background on the origin and the development of the two proposed legislative texts. These two proposed legislative texts include:

- A proposed Regulation: *General Data Protection Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, which will supersede Directive 95/46/EC; and

- A proposed Directive: *Police and Criminal Justice Data Protection Directive 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 offenses or the execution of criminal penalties, and the free movement of such data*.

The Proposed Regulation and Proposed Directive will now be discussed by the European Parliament and EU Member States meeting in the Council of Ministers.[26] Thus, there will be more opportunities for discussion and modifications of the current provisions, and it is uncertain whether or to which extent the provisions as stated in the January 25, 2012 draft will remain or how they will be modified.

Given the energy, speed, and determination with which the reform of the EU data protection regime has been handled,[27] it is likely that a final vote will take place sooner than later. The final

---

25. *Safeguarding Privacy*, *supra* note 6.

26. *See generally* GILBERT, *supra* note 3, at 4-26 to 4-27 ("Decision-Making Process"); KLAUS-DIETER BORCHARDT, THE ABC OF EUROPEAN UNION LAW 98-102 (2010), *available at* http://bookshop.europa.eu/uri?target=EUB:NOTICE:OA8107147:EN.

27. *See Proposed Regulation*, *supra* note 1, at 2-5 (summarizing the main developments, including a high level personal data conference in May 2009, two phases of public consultation in 2009 and 2010-2011, the Commission's call for a revision of the 2008/977/JHA Framework Decision in late 2009, the EU Communication "A comprehensive approach on personal data protection in the European Union" in 2010, numerous roundtable discussions, conferences, workshops, stakeholder consultation meetings at the EU Commission or agency level in 2011, along with the results from various commissioned studies and impact assessment analyses.).

legislative texts are expected to take effect two years after their formal adoption by the European Parliament.[28] Thus, it is likely that, by 2015, the European Economic Area will be subject to a new, improved, but stricter data protection regime.

This article discusses only the Proposed Regulation. In the first part, after providing the necessary historical and legal background to understand the genesis and nature of the proposed document, we analyze and discuss the provisions of the January 25, 2012 draft of the Proposed Regulations. Then we analyze whether the initial goal of uniformity and consistency might be derailed by several provisions of the Proposed Regulation that grant Member States extensive powers to carve out and make restrictions or add new provisions to the common rule.

2. BACKGROUND; EU LAW BASICS

Before delving into the detailed analysis of the provisions of the proposed document, it is important to look at the historical background and the unique rules of operation of the European Union. Both of these explain the choices made, and the intent of the drafters.

2.1 Historical Milestones

The European Union is over 50 years old.[29] For a long time, the Union functioned as a group of countries operating under a set of rules that attempted to be consistent with each other, in order to ease the flow of people and goods among the Member States.[30] This was achieved by implementing numerous directives on a piecemeal basis.[31] When implementing the directives, each Member State

---

28. *Proposed Regulation*, *supra* note 1, art. 91(2), at 99 (providing that the proposed regulation shall be enforced two years from its publication in the Official Journal of the European Union).

29. *See* GILBERT, *supra* note 3, at 4-5 ("The European Union is a complex international organization of sovereign states . . . . The principal rules of operations are found in several treaties, such as the Treaty of Rome (1957), the Treaty of Maastricht (1992), or the Treaty of Lisbon (2009)."); *see also Basic Information on the European Union*, EUROPA, http://europa.eu/about-eu/basic-information/index_en.htm ("The European Union is a unique economic and political partnership between 27 European countries . . . . It has delivered half a century of peace, stability, and prosperity, helped raise living standards, and launched a single European currency.").

30. *See* GILBERT, *supra* note 3, at 4-16 ("The European Union only deals with the issues for which it was granted responsibility by the Member States. It only has the power to tell the governments of its Member States what to include in some of their laws in order to ensure the free movement of goods, services, people, and money throughout the European Union.").

31. *See id.* at 4-29 to 4-30 ("EU Directives are pieces of European legislation that are

retained—or elected to take—a lot of independence and autonomy.[32] While this strategy created a sense of unity among countries that had different cultures, history and personalities, it ended up creating a patchwork of national laws that had some resemblance to the base directive, but also distinct personalities.[33] These inconsistencies and discrepancies have created a difficult setting for companies operating in several Member States.[34]

Some of this changed with the ratification of the Treaty of Lisbon in late 2009.[35] It marked a critical step in the evolution of the Union by creating deep changes in its rules of operation.[36] It also removed the three-pillar system that fragmented the operations,[37] and

---

addressed to the Member States. Once a directive is passed at the European Union level, each Member State must ensure that the directive is effectively implemented in its legal system. Unlike regulations, which become part of the national legal systems of all Member States automatically, without the need for separate national legal measures, Directives require that each national government take action to "implement" or "transpose" the Directive into its national law."); *id.* at 4-31 to 4-32 (examples of directives pertaining to personal data); *see also id.* at 5-3.

32. *See generally* GILBERT, *supra* note 3 (Chapter 13 "Austria," Chapter 14 "Belgium," Chapter 16 "Bulgaria," Chapter 21 "Cyprus," Chapter 22 "Czech Republic," Chapter 23 "Denmark," Chapter 26 "Estonia," Chapter 27 "Finland," Chapter 28 "France," Chapter 29 "Germany," Chapter 30 "Greece," Chapter 32 "Hungary," Chapter 35 "Ireland," Chapter 37 "Italy," Chapter 39 "Latvia," Chapter 41 "Lithuania," Chapter 42 "Luxembourg," Chapter 44 "Malta," Chapter 46 "The Netherlands," Chapter 49 "Poland," Chapter 50 "Portugal," Chapter 51 "Romania," Chapter 54 "Slovakia," Chapter 55 "Slovenia," Chapter 58 "Spain," Chapter 59 "Sweden," Chapter 64 "United Kingdom," describing the data protection laws adopted by each EU Member State).

33. *See* GILBERT, *supra* note 3, at 4-30 to 4-31 ("Each Member State may add to the principles in the directive by imposing country-specific requirements, or adding concepts. . . . Further, some provisions of a directive may give the Member States the choice whether to adopt a provision."); *id.* at 4-38 ("Despite a common history, and the appearance of a single regime under the Directive, the data protection laws of the European Union Member States are not uniform. Although there are significant similarities, there are drastic differences in the application of these laws, as well in the administrative and implementation details.").

34. *See id.* at 4-38 to 4-40 ("Companies doing business in Europe should keep in mind the tremendous discrepancies between the treatment of personal information throughout the European Union and outside of this group of countries.").

35. Treaty of Lisbon Amending the Treaty on European Union and the Treaty Establishing the European Communities, Dec. 13, 2007, 2007 O.J. (C 306) 1, http://europa.eu/lisbon_treaty/full_text/index_en.htm. *See also Treaty of Lisbon*, EUROPA, http://europa.eu/lisbon_treaty/countries/index_en.htm ("The Treaty of Lisbon, officially signed by the Heads of the Member States on 13 December 2007, entered into force on 1 December 2009.").

36. GILBERT, *supra* note 3, at 4-20 to 4-21; BORCHARDT, *supra* note 26, at 13 ("[The Treaty of Lisbon] made fundamental changes to the existing EU Treaties in order to strengthen the EU's capacity to act within and outside the Union, increase its democratic legitimacy and enhance the efficiency of EU action overall.").

37. GILBERT, *supra* note 3, at 4-18 n.25 ("The three-pillar structure was abolished by the

moved the federation into a tighter structure.[38]

In November 2010, taking advantage of the new structure and new expanded powers, the European Commission published a document that outlined its plans to reform the data protection regime in the European Union to conform to the new structures created by the Treaty of Lisbon.[39] Most of the key elements described in the November 2010 document that presented the blue print for the reform are found in the proposed legislative text published in January 2012.[40]

2.2 Regulation v. Directive

With this background in mind, it is logical that the European Commission found that a "regulation," as opposed to a "directive," was the most appropriate legal instrument to define the new framework for regulating the processing of personal data by companies and government agencies in their day-to-day operations. EU regulations are the most direct form of EU law.[41] As soon as a regulation is passed, it automatically becomes part of the national legal system of each Member State.[42]

---

ratification of the Treaty of Lisbon in 2009."); BORCHARDT, *supra* note 26, at 16 ("The Treaty of Lisbon also abandons the EU's 'three pillars'. The first pillar, consisting essentially of the single market and the EC policies, is merged with the second pillar, consisting of the common foreign and security policy, and the third pillar, covering police and judicial cooperation in criminal matters.").

38. BORCHARDT, *supra* note 26, at 14 ("The Treaty of Lisbon merges the European Union and the European Community into a single European Union.").

39. *Communication 609*, *supra* note 5, at 4. ("The Lisbon Treaty provided the EU with additional means to achieve [data protection for individuals]: the EU Charter of Fundamental Rights—with Article 8 recognising an autonomous right to the protection of personal data—has become legally binding, and a new legal basis has been introduced allowing for the establishment of comprehensive and coherent Union legislation on the protection of individuals with regard to the processing of their personal data and on the free movement of such data. In particular, the new legal basis allows the EU to have a single legal instrument for regulating data protection, including the areas of police cooperation and judicial cooperation in criminal matters.").

40. *See generally Communication 609*, *supra* note 5; *Proposed Regulation*, *supra* note 1.

41. Consolidated Version of the Treaty on the Functioning of the European Union art. 288, May 9, 2008, 2008 O.J. (C 115) 171 [hereinafter TFEU] ("A regulation shall have general application. It shall be binding in its entirety and directly applicable in all Member States."). *Accord* GILBERT, *supra* note 3, at 4-29 ("EU Regulations are the most direct form of EU law."); BORCHARDT, *supra* note 26, at 88-89 ("[Regulations] lay down the same law throughout the Union, regardless of international borders, and apply in full in all Member States.").

42. GILBERT, *supra* note 3, at 4-29 ("As soon as they are passed, the EU Regulations become part of the national legal systems automatically . . . ."); *see also EUR-Lex: Access to European Union Law: Process and Players*, EUROPA,

http://eur-lex.europa.eu/en/droit_communautaire/droit_communautaire.htm (last updated Aug. 6, 2008) ("A regulation is directly applicable, which means that it creates law which takes

EU directives, on the other end, are used to bring different national laws in-line with each other.[43] Once a directive is passed at the European Union level, each Member State must implement or "transpose" the directive into its legal system, but can do so in its own words.[44] A directive only takes effect through national legislation that implements the measures.[45]

The current data protection regime, which is based on a series of directives—in particular, Directive 95/46/EC, Directive 2002/58/EC (as amended) and Directive 2006/24/EC—has proved to be very cumbersome due to the significant discrepancies between the interpretations or implementations of each directive that were made in the various Member States.[46] When developing or revising their data protection laws, the 27 Member States created a patchwork of 27 rules with different structures, different wording, and even different basic rules.[47] This fragmentation creates a significant burden on

---

immediate effect in all the Member States in the same way as a national instrument, without any further action on the part of the national authorities.").

43. GILBERT, *supra* note 3, at 4-29 ("The EU Directives are used to bring different national laws in line with each other."); BORCHARDT, *supra* note 26, at 89 ("[The] purpose [of the directive] is to reconcile the dual objectives of both securing the necessary uniformity of Union law and respecting the diversity of national traditions and structures. What the directive primarily aims for, then, is not the unification of the law, which is the regulation's purpose, but its harmonisation. The idea is to remove contradictions and conflicts between national laws and regulations or gradually iron out inconsistencies so that, as far as possible, the same material conditions exist in all the Member States.").

44. GILBERT, *supra* note 3, at 4-29 to 4-30 ("Once a directive is passed at the European Union level, each Member State must . . . 'implement' or 'transpose' the Directive into its national law."); BORCHARDT, *supra* note 26, at 89 ("A directive is binding on the Member States as regards the objective to be achieved but leaves it to the national authorities to decide on how the agreed Community objective is to be incorporated into their domestic legal systems.").

45. GILBERT, *supra* note 3, at 4-30; BORCHARDT, *supra* note 26, at 90 ("Directives do not as a rule directly confer rights or impose obligations on the Union citizen. They are expressly addressed to the Member States alone. Rights and obligations for the citizen flow only from the measures enacted by the authorities of the Member States to implement the directive.").

46. GILBERT, *supra* note 3, at 4-35 to 4-38; *id.* at 5-3 to 5-4. *See also Safeguarding Privacy*, *supra* note 6, at 7 ("Despite the current Directive's objective to ensure an equivalent level of data protection within the EU, there is still considerable divergence in the rules across Member States. As a consequence, data controllers may have to deal with 27 different national laws and requirements. The result is a fragmented legal environment which has created legal uncertainty and uneven protection for individuals."); *Proposed Regulation*, *supra* note 1, at 18 ("This difference in levels of [personal data] protection is due to the existence of differences in the implementation and application of Directive 95/46/EC.").

47. *Proposed Regulation*, *supra* note 1, at 18. *See also Impact Assessment Report*, *supra* note 17, at 13 ("As a consequence, key provisions and concepts have been interpreted and transposed in quite different ways by Member States, so that the same processing is treated divergently across Member States and thus impacts cross-border processing activities by public authorities and businesses.").

businesses, which are forced to act as chameleons and adapt to the different privacy rules of the countries in which they operate, or risk retaliation by the national data protection supervisory authorities.[48]

Conversely, a regulation is the law as written, in the Member States.[49] By adopting a Regulation for data protection matters, the EU Commission intends to equip each of its Member States with the same basic legal instrument that applies uniformly.[50] The choice of a regulation for the new general regime for personal data protection should provide greater legal certainty by introducing a harmonized set of core rules that will be the same in each Member State.

While on paper this Proposed Regulation should instill more uniformity amongst the Member States, it remains to be seen how fiercely independent countries, judges, lawyers or government officials will implement or interpret it. Further, there are numerous circumstances—described in the last section of this article—where the Proposed Regulation would grant Member States the ability to enact their own rules or laws.[51] This additional freedom is likely to be used, especially in those countries that have already expressed reservations on the content and substance of the Proposed Regulation.[52]

---

48. *See Impact Assessment Report*, *supra* note 17, at 19 ("As the [95/46EC] Directive leads to the simultaneous application of national laws where the controller is established in several Member States, data controllers operating across borders need to spend time and money . . . to comply with different, and sometimes contradictory, obligations, such as the different requirements for notifications of data processing to DPAs.").

49. *See supra* note 41.

50. *Proposed Regulation*, *supra* note 1, at 5-6 ("A Regulation is considered to be the most appropriate legal instrument to define the framework for the protection of personal data in the Union. The direct applicability of a Regulation in accordance with Article 288 TFEU will reduce legal fragmentation and provide greater legal certainty by introducing a harmonised set of core rules, improving the protection of fundamental rights of individuals and contributing to the functioning of the Internal Market.").

51. *See supra* Part 0. *See also, e.g.*, *Proposed Regulation*, *supra* note 1, at 15, 94-95 (Article 80 empowers Member States to adopt exemptions where necessary to reconcile the right to the protection of personal data with the right of freedom of expression); *id.* at 15-16, 95-97 (Articles 81-82, empowering Member States to enact specific laws to safeguard the processing of health information and ensure the protection of employee personal data in the employment context, and Articles 84-85, to adopt rules regarding interaction with professionals having an obligation of secrecy and the collection of personal data by churches and religious associations).

52. *See, e.g.*, Bloomberg BNA, *CNIL Opposes EC Data Regulation; Says Would Undercut National DPAs*, 11 PRIVACY & SECURITY LAW REPORT 1, 3 (Jan. 30, 2012); ("France's data protection authority (CNIL) firmly opposes the European Commission's proposed data protection regulation because it would 'largely deprive citizens of protection offered by their national authorities . . .'"); *Initial response from the ICO on the European Commission's Proposal for a New General Data Protection Regulation*, INFORMATION COMMISSIONER'S OFFICE, UNITED KINGDOM (Jan. 25, 2012),
http://www.ico.gov.uk/news/latest_news/2012/statement-initial-response-new-data-protection-

The Proposed Regulation provides for checks and balances in the form of cooperation and oversight so that the discrepancies between these interpretations should be less significant than those that are currently found among the Member State data protection laws.[53] Nevertheless, it would be very risky to act as if there were total uniformity.

3. OVERVIEW OF THE PROPOSED REGULATION

The 119-page Proposed Regulation lays out the proposed new rules. Among the most significant changes, the Proposed Regulation would change the consent process to require that there be an "explicit" consent.[54] The Draft introduces some new concepts that were not in Directive 95/46/EC,[55] such as: the concept of breach of security,[56] the protection of the personal information of children,[57] the use of binding corporate rules,[58] the special status of health

---

regulation-proposals-25012012.aspx ("[T]he Commissioner believes that in a number of areas the proposal is unnecessarily and unhelpfully over prescriptive. . . . The proposal also fails to properly recognise the reality of international transfers of personal data in today's globalised world . . . .").

53. *See Proposed Regulation*, *supra* note 1, art. 55(1), at 80 ("Supervisory authorities shall provide each other relevant information and mutual assistance in order to implement and apply this Regulation in a consistent manner, and shall put in place measures for effective co-operation with one another."); *id.*, art. 64, at 86 (establishing a European Data Protection Board "composed of the head of one supervisory authority of each Member State and of the European Data Protection Supervisor"); *id.*, arts. 57-58, at 82-83 (providing a consistency mechanism to "ensure correct and consistent application of this Regulation").

54. *Proposed Regulation*, *supra* note 1, art. 4(8), at 42 (defining 'the data subject's consent' as "any freely given specific, informed and explicit indication of his or her wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed"); *id.* at 8 ("In the definition of consent, the criterion 'explicit' is added to avoid confusing parallelism with 'unambiguous' consent and in order to have one single and consistent definition of consent, ensuring the awareness of the data subject that, and to what, he or she gives consent.").

55. For a detailed analysis of Directive 95/46/EC, *see generally* GILBERT, note 3 *supra*, ch. 4-6, 9 (chapter 4 "The Byzantine Process of European Data Protection Law Making;" chapter 5 "Introduction to the European Union Directives;" chapter 6 "The 1995 EU Data Protection Directive;" and chapter 9 "Transferring Personal Data out of the European Union and the European Economic Area").

56. *Proposed Regulation*, *supra* note 1, art. 4(9), at 42 (defining a 'personal data breach' as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed").

57. *Proposed Regulation*, *supra* note 1, art. 8, at 45 ("the processing of personal data of a child below the age of 13 years shall only be lawful if and to the extent that consent is given or authorised by the child's parent or custodian."). *See also id.*, Preamble Recital at 22-24 (paras. 29, 38, 46).

58. *Proposed Regulation*, *supra* note 1, arts. 42-43, at 70-72 (providing binding corporate

information,[59] or the requirement for a data protection officer for most corporations and government agencies.[60] It would also require companies to conduct privacy impact assessments,[61] to implement "Privacy by Design" rules,[62] and to ensure "Privacy by Default" in their application.[63] Individuals would have greater rights, such as the "Right to be Forgotten"[64] and the "Right to Data Portability."[65] Some of the key components of the Proposed Regulation are discussed below.

3.1 New, Expanded Data Protection Principles

Articles 5 through 7 would incorporate the general principles governing personal data processing that were laid out in Article 6 of Directive 95/46/EC.[66] New elements would be added, such as: the requirement for increased transparency, the establishment of a comprehensive responsibility and liability of the controller, and the clarification of the data minimization principle.[67] The seven basic

---

rules as appropriate safeguards to be used in transfers to third countries).

59. *Proposed Regulation*, *supra* note 1, at 36 (Preamble Recital paragraph 122 treats the processing of personal data concerning health as a special category of data deserving of higher protection); *id.*, art. 9, at 45-46 (prohibiting processing of data concerning health except under ten specially enumerated circumstances).

60. *Proposed Regulation*, *supra* note 1, art. 35(1), at 65 (requiring designation of a data protection officer where data processing is carried out by a public authority, by an enterprise employing 250 persons or more, or if the core activities of the controller or the processor "consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects.").

61. *Proposed Regulation*, *supra* note 1, art. 33(1), at 62 (requiring an impact assessment of the proposed processing operations where "processing operations present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes").

62. *Proposed Regulation*, *supra* note 1, at 27 (Preamble Recital paragraph 61: "In order to ensure and demonstrate compliance with this Regulation, the controller should adopt internal policies and implement appropriate measures, which meet in particular the principles of data protection by design and data protection by default."); *id.*, art. 23, at 56 ("Data protection by design and by default").

63. *Proposed Regulation*, *supra* note 1, at 27 and text accompanying note 62; *id.*, art. 23, at 56 and text accompanying note 62.

64. *Proposed Regulation*, *supra* note 1, at 9 ("Article 17 provides the data subject's right to be forgotten and to erasure. It further elaborates and specifies the right of erasure provided for in Article 12(b) of Directive 95/46/EC . . . ."); *id.* at 51-53 (text of Articles 17 and 18).

65. *Id.* at 53 (Article 18(1) entitles the data subject "to obtain from the controller a copy of data undergoing processing in an electronic and structured format which is commonly used and allows for further use by the data subject.").

66. *See generally* GILBERT, *supra* note 3, at 6-1 to 6-54 (Chapter 6, "The 1995 EU Data Protection Directive").

67. *Proposed Regulation*, *supra* note 1, at 8 ("Article 5 sets out the principles relating to personal data processing, which correspond to those in Article 6 of Directive 95/46/EC. Additional new elements are in particular the transparency principle, the clarification of the data

principles relating to data processing would require that the personal data be:

- Processed lawfully, fairly, and in a transparent manner;
- Collected for specified, explicit, and legitimate purposes, and not further processed in ways incompatible with these purposes;
- Adequate, relevant and limited to the minimum necessary;
- Only processed if, and as long as, the purposes of the processing could not be fulfilled by processing information that does not involve personal data;
- Accurate, kept up-to-date, with incorrect data being erased or rectified;
- Kept in a form that permits identification of the data subjects for no longer than necessary;
- Processed under the responsibility and liability of the data controller, who must ensure and demonstrate for each operation its compliance with the Regulation.[68]

3.1.1 Specific, Informed and Explicit Consent

One of the significant differences with Directive 95/46/EC is that the notion of consent is strengthened.[69] Currently, in many EU Member States, consent is implied in many circumstances.[70] For

---

minimisation principle and the establishment of a comprehensive responsibility and liability of the controller."); *id.* at 43 (text of Article 5).

68. *Proposed Regulation*, *supra* note 1, art. 5(a)-(f), at 43.

69. *See Safeguarding Privacy*, *supra* note 6, at 6 (The proposed rules will "[i]mprove individuals' ability to control their data, by: ensuring that, when their consent is required, it is given explicitly, meaning that it is based either on a statement or on a clear affirmative action by the person concerned and is freely given;").

70. *See* Annexes to *Impact Assessment Report*, *supra* note 17, Annex 2 at 10, *available at* http://ec.europa.eu/justice/data-protection/document/review2012/sec_2012_72_annexes_en.pdf ("[S]ome other Member States (e.g. France, Ireland, Romania and UK) do not provide a definition of 'consent' in their national data protection laws. In practice, this leaves room for considering, in certain circumstances, that "consent" to the processing of (non-sensitive) data is implied, as it is the case in the UK. In some cases it is not even clear what would constitute

example, in most countries, an individual who uses a website is often assumed to have agreed to the privacy policy of that website.[71]

Under the new regime, when consent is the basis for the legitimacy of the processing, it will have to be "specific, informed, and explicit".[72] The controller would bear the burden of proving that the data subjects gave their consent to the processing of their personal data for specified purposes.[73] For companies, this means that they may have to find ways to keep track of the consent received from their customers, users, visitors and other data subjects, or will be forced to ask for this consent each time the company receives any data.

This evolution is consistent with the way cookies are treated under the 2009 amendments to Directive 2002/58/EC.[74] As a result of these amendments many of the EU Member States have modified their national laws to require that the user's specific opt-in consent be obtained before cookies, other than "strictly necessary" cookies, can be sent to the user's browser.[75]

---

freely given, specific and informed consent to data processing.").

71. *See, e.g.*, Bank of America Privacy & Security, BANK OF AMERICA (Mar. 2, 2012), http://www.bankofamerica.com/privacy ("By using our Site, you agree to the terms and conditions of this Notice."); Amazon.com Privacy Notice, AMAZON.COM (Apr. 6, 2012), http://www.amazon.com/gp/help/customer/display.html/ref=footer_privacy?ie=UTF8&nodeId=468496 ("By visiting Amazon.com, you are accepting the practices described in this Privacy Notice.").

72. *Proposed Regulation*, *supra* note 1, art. 4(8), at 42 (defining 'the data subject's consent' as "any freely given specific, informed and explicit indication of his or her wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed").

73. *Id.*, art. 7(1), at 45 ("The controller shall bear the burden of proof for the data subject's consent to the processing of their personal data for specified purposes.").

74. *See* GILBERT, *supra* note 3, at 7-4 to 7-5 ("The 2002 Directive, as amended by the 2009 Directive, defines rules for the use of cookies. Since cookies are used to collect personal information, their use should be subject to the same rules on notice and choice defined in the 1995 Data Protection Directive. To this end, the 2002 Directive, as amended, requires that users give their consent to the use of cookies."). *See generally id.* at 7-1 to 7-30 (Chapter 7 "The 2002 EU Directive on Privacy and Electronic Communications").

75. *See, e.g.*, U.K. INFORMATION COMMISSIONER'S OFFICE, GUIDANCE ON THE RULES ON USE OF COOKIES AND SIMILAR TECHNOLOGIES (2011), *available at* http://www.ico.gov.uk/for_organisations/privacy_and_electronic_commusnications/the_guide/~/media/documents/library/Privacy_and_electronic/Practical_application/guidance_on_the_new_cookies_regulations.ashx ("Since 2003 anyone using cookies has been required to provide clear information about those cookies. In May 2011 the existing rules were amended. Under the revised Regulations the requirement is not just to provide clear information about the cookies but also to obtain consent from users or subscribers to store a cookie on their device."); The Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011, 2011, S.I. 2011/1208, art. 6 at 3-4. (U.K.), *available at*

3.2 Special Categories of Processing

The rules that apply to special categories of processing would be expanded. In the January 25, 2012 draft, these rules are found in Articles 8 through 10 and in Articles 80 through 85.

3.2.1 Protection of Children Under 13

Article 8 sets out the conditions for the lawfulness of the processing of data about children in relation to information society services directly offered to them.[76] The term "child" would be defined as an individual under 13 years of age.[77] In the prior draft, Draft 56, dated November 29, 2011, the age limit was 18.[78] The change to 13 is consistent with the definition in the United States COPPA law, which also protects the rights of young individuals.[79]

3.2.2 Expanded Definition of Sensitive Data

The definition of "sensitive data" would be expanded to include genetic data and criminal convictions or related security measures.[80] The notion of what constitutes "sensitive data" would continue to be significantly different from that of the United States. In the United States, data that is generally identified as "sensitive" tends to be data that would result in identity theft in case of a loss or breach of

---

http://www.legislation.gov.uk/uksi/2011/1208/pdfs/uksi_20111208_en.pdf
(amending regulation 6 of Privacy and Electronic Communications (EC Directive) Regulations 2003, 2003, S.I. 2003/2426 (U.K.), *available at*
http://www.legislation.gov.uk/uksi/2003/2426/pdfs/uksi_20032426_en.pdf, to require consent from users or subscribers to store a cookie on their device).

76. *Proposed Regulation*, *supra* note 1, art. 8(1), at 45 ("For the purposes of this Regulation, in relation to the offering of information society services directly to a child, the processing of personal data of a child below the age of 13 years shall only be lawful if and to the extent that consent is given or authorised by the child's parent or custodian.").

77. *Id. But see id.*, art. 4(18), at 43 (defining 'child' as "any person below the age of 18 years").

78. *Commission Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data (General Data Protection Regulation)*, art. 3(18), at 38, COM (2011) 56 draft (Nov. 29, 2011) [hereinafter *Draft 56 of Proposed Regulation*], *available at* http://statewatch.org/news/2011/dec/eu-com-draft-dp-reg-inter-service-consultation.pdf
(defining 'child' as "any person below the age of 18 years").

79. *See* Child Online Privacy Protection Act, 15 U.S.C. § 6501(1) (2006) (defining the term 'child' as "an individual under the age of 13").

80. *Proposed Regulation*, *supra* note 1, art. 9, at 45 (providing the "processing of personal data, revealing race or ethnic origin, political opinions, religion or beliefs, trade-union membership, and the processing of genetic data or data concerning health or sex life or criminal convictions or related security measures shall be prohibited.").

security; for example, credit card or driver's license information.[81] In the European Union, data that is deemed "sensitive" is data that might cause embarrassment or intrusion into a person's intimate life if the data were lost or exposed, such as data about health or sexual preference or that may cause discrimination or retaliation, such as data about religion or trade union membership.[82]

3.2.3 Additional Exceptions

Articles 80 to 85 would provide additional rules with respect to certain categories of processing. Some of these categories of data, such as health data or data collected by churches were not specifically regulated under Directive 95/46/EC.[83] The special categories would include processing of personal data for:

- Journalistic purposes;
- Health purposes;
- Use in the employment context;
- Historical, statistical or scientific purposes;
- Access by a data protection authority to personal data and premises where data controllers are subject to an obligation of secrecy; and
- Churches.[84]

For these specific types of data, Member States would have the freedom to enact their own laws, consistent with their own culture and past practices.

---

81. *See, e.g.*, CAL. CIV. CODE § 1798.29(e) (listing what kind of information, if compromised as a result of a breach of security, requires a data breach notification).

82. Council Directive 95/46/EC, *supra* note 9, art. 8(1), 1995 O.J. (L 281) 40.

83. *See generally* GILBERT, *supra* note 3, at 6-1 to 6-53 (Chapter 6, "The 1995 EU Data Protection Directive").

84. *Proposed Regulation*, *supra* note 1, art. 80, at 94-97.

3.3 Crossborder Data Transfers

For most global companies, a critical aspect of compliance with the EU data protection laws requires understanding in what way the national law of a country restricts the transfer of personal data out of the country. Under current national data protection laws, which are based on Directive 95/46/EC, the transfer of personal information out of the European Economic Area and to most of the rest of the world is prohibited unless an exception applies.[85] This rule remains in the Proposed Regulation.[86] However, the Proposed Regulation would provide for simplification in the form of a "one-stop shop" approach for larger companies,[87] remove the discrepancies in the regimes for cross-border data transfers,[88] and validate the use of binding corporate rules.[89]

In the new Regulation Articles 40 through 45 define the conditions of, and restrictions to, data transfers to third countries or international organizations, including onward transfers. For transfers to third countries that have not been deemed to provide "adequate protection," Article 42 would require that the data controller *or data*

---

85. *See* Council Directive 95/46/EC, *supra* note 9, art. 26, 1995 O.J. (L 281) 46 (permitting the transfer of personal data to third countries which do not "ensure an adequate level of protection" under six enumerated exceptions, or if the controller "adduces adequate safeguards . . . such [as] . . . appropriate contractual clauses."). *See generally* GILBERT, *supra* note 3, 6-1 to 6-54, 9-1 to 9-79 (chapter 6 "The 1995 EU Data Protection Directive" and chapter 9 "Transferring Personal Data out of the European Union and the European Economic Area").

86. *Proposed Regulation*, *supra* note 1, arts. 42-44, at 70-74 (permitting personal data transfers to third countries without an adequacy decision only if the controller adduces appropriate safeguards by standard data protection clauses, binding corporate rules or contractual clauses, or under eight enumerated exceptions).

87. *Id.* at 12 ("Article 51 sets out the competence of the supervisory authorities. The general rule, based on Article 28(6) of Directive 95/46/EC (competency on the territory of its own Member State), is complemented by the new competence as lead authority in case that a controller or processor is established in several Member States, to ensure unity of application ('one-stop shop')."); *id.* at 32 (providing that the supervisory authority of the Member State in which the controller or processor has its main establishment is the one-stop shop for "monitoring the activities of the controller or processor throughout the Union and taking the related decisions, in order to increase the consistent application, provide legal certainty and reduce administrative burden for such controllers and processors.").

88. *Proposed Regulation*, *supra* note 1, art. 44, at 73 ("In the absence of an adequacy decision pursuant to Article 41 or of appropriate safeguards pursuant to Article 42, a transfer or a set of transfers of personal data to a third country or an international organisation may take place only on" certain conditions.).

89. *Id.*, art. 42(2)(a), at 70 ("The appropriate safeguards referred to in paragraph 1 shall be provided for, in particular, by: (a) binding corporate rules in accordance with Article 43."); *id.*, art. 43, at 71-73 (setting forth conditions for transfers to third countries by way of binding corporate rules).

processor adduce appropriate safeguards, such as through standard data protection clauses, binding corporate rules, or contractual clauses. It should be noted, in particular, that:

- Standard data protection clauses may be adopted by a supervisory authority and be declared generally valid by the Commission;[90]

- Binding corporate rules are specifically introduced as a legitimate ground for allowing for the transfer of personal information out of the European Economic Area.[91] Currently they are only accepted or recognized in about twenty-one Member States;[92]

- The use of contractual clauses other than the standard clauses would be subject to prior authorization by the supervisory authorities.[93]

Binding Corporate Rules take a prominent place in the Proposed Regulation, while they were not mentioned in Directive 95/46/EC. Article 43 lays out in further detail the conditions for transfers by way of binding corporate rules and outlines the required content of binding corporate rules. Article 44 spells out and clarifies the derogations for a data transfer. These conditions are based on Article 26 of Directive

---

90. *Id.*, art. 42(2)(c), at 70-71 ("The appropriate safeguards referred to in paragraph 1 shall be provided for, in particular, by: . . . (c) standard data protection clauses adopted by a supervisory authority in accordance with the consistency mechanism referred to in Article 57 when declared generally valid by the Commission pursuant to point (b) of Article 62(1).").

91. *See id.*, art. 42(1), at 70 ("[A] controller or processor may transfer personal data to a third country or an international organization only if the controller or processor has adduced appropriate safeguards with respect to the protection of personal data in a legally binding instrument."); *id.*, art. 42(2)(a), at 70 ("The appropriate safeguards referred to in paragraph 1 shall be provided for, in particular, by: (a) binding corporate rules in accordance with Article 43.").

92. *What is Mutual Recognition*, EUROPEAN COMMISSION, http://ec.europa.eu/justice/data-protection/document/international-transfers/binding-corporate-rules/mutual_recognition/index_en.htm (last visited Aug. 10, 2012). *See also* GILBERT, *supra* note 3, at 9-56 to 9-57; *Overview on Binding Corporate Rules*, EUROPEAN COMMISSION, http://ec.europa.eu/justice/data-protection/document/international-transfers/binding-corporate-rules/index_en.htm (last visited Aug. 10, 2012).

93. *Proposed Regulation*, *supra* note 1, art. 42(4), at 71 ("Where a transfer is based on contractual clauses . . . the controller or processor shall obtain prior authorization of the contractual clauses . . . from the supervisory authority.").

95/46/EC.[94] In addition, under limited circumstances, a data transfer may be justified on a legitimate interest of the controller or processor, but only after having assessed and documented the circumstances of the proposed transfer.[95]

Article 45 provides for international cooperation mechanisms for the protection of personal data between the European Commission and the supervisory authority of third countries. It should be noted that Article 42 of the prior draft of the Regulation has been removed.[96] That article provided that foreign judgments requiring a controller or processor to disclose personal data were not enforceable in any manner; except in the case of mutual assistance treaties or an international agreement in force between the requesting third country and the Union or a Member State.[97] It also required a controller or processor to immediately notify the supervisory authority of the request and to obtain authorization for the transfer before it occurred.[98] It is not clear why the provision was removed and whether this issue will be addressed separately.

---

94. *See generally* GILBERT, *supra* note 3, 6-1 to 6-53, 9-1 to 9-79 (chapter 6 "The 1995 EU Data Protection Directive" and chapter 9 "Transferring Personal Data out of the European Union and the European Economic Area").

95. *Proposed Regulation*, *supra* note 1, at 73 (Article 44(1)(h) provides that absent an adequacy decision or appropriate safeguards, "a transfer or a set of transfers of personal data to a third country or an international organisation may take place only on condition that: . . . (h) the transfer is necessary for the purposes of the legitimate interests pursued by the controller or the processor, which cannot be qualified as frequent or massive, and where the controller or processor has assessed all the circumstances surrounding the data transfer operation or the set of data transfer operations and based on this assessment adduced appropriate safeguards with respect to the protection of personal data, where necessary."); *id.* at 74 (Article 44(6) provides "[t]he controller or processor shall document the assessment as well as the appropriate safeguards adduced . . . in the documentation . . . and shall inform the supervisory authority of the transfer.").

96. *Draft 56 of Proposed Regulation*, *supra* note 78, at 69 (Article 42 prohibiting controllers operation in the EU from disclosing personal data to a third country even when requested by that country's judicial or administrative authority, unless expressly authorized by an international agreement, mutual legal assistance treaties, or approved by a supervisory authority).

97. *Draft 56 of Proposed Regulation*, *supra* note 78, at 69 (Article 42(1) provided "[n]o judgment of a court or tribunal and no decision of an administrative authority of a third country requiring a controller or processor to disclose personal data shall be recognized or be enforceable in any manner, without prejudice to a mutual assistance treaty or an international agreement in force between the requesting third country and the Union or a Member State.").

98. *Draft 56 of Proposed Regulation*, *supra* note 78, at 69 (Article 42(2) provided "[w]here a judgment of a court or tribunal or a decision of an administrative authority of a third country requests a controller or processor to disclose personal data, the controller or processor and, if any, the controller's representative, shall notify the supervisory authority of the request without undue delay and must obtain prior authorisation for the transfer by the supervisory authority in accordance with point (b) of Article 31(1).").

3.4 Obligations of Controllers and Processors

Articles 22 through 29 define the obligations of the controllers and processors, as well as those of the joint controllers and the representatives of controllers that are established outside of the European Union.

3.4.1 Accountability

Article 22 addresses the accountability of the controllers. This concept is a new one, and resembles the concept of accountability found in the APEC Privacy Framework.[99]

The Proposed Regulation would require "the [data] controller [to] adopt policies and implement appropriate measures to ensure and be able to demonstrate that the processing of personal data is performed in compliance with [the] Regulation."[100] These measures would include the following obligations for the data controller:

- The obligation to keep documents;[101]
- The obligation to implement data security measures;[102]

---

99. *Compare* ASIA-PACIFIC ECONOMIC CORPORATION (APEC): PRIVACY FRAMEWORK (2005), 28, *available at* http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx ("A personal information controller should be accountable for complying with measures that give effect to the Principles stated above. When personal information is to be transferred to another person or organization, whether domestically or internationally, the personal information controller should obtain the consent of the individual or exercise due diligence and take reasonable steps to ensure that the recipient person or organization will protect the information consistently with these Principles.") *with Proposed Regulation*, *supra* note 1, at 10 ("Article 22 takes account of the debate on a "principle of accountability" and describes in detail the obligation of responsibility of the controller to comply with this Regulation and to demonstrate this compliance, including by way of adoption of internal policies and mechanisms for ensuring such compliance."). *See also* GILBERT, *supra* note 3,10-1 to 10-19.

100. *Proposed Regulation*, *supra* note 1, art. 22(1), at 55.

101. *Proposed Regulation*, *supra* note 1, art. 22(2)(a), at 55 (including as an appropriate measure "keeping the documentation pursuant to Article 28"). *See also id.*, art. 28(2), at 58-59 (requiring documentation on the names and contact details of the controller and data protection officer (if any), purposes of the processing, categories of data subjects and the categories of personal data relating to them; the recipients or categories of recipients of the personal data, transfers of data to a third country, including any appropriate safeguards, time limits for erasure for the different categories of data, and the mechanisms by which the controller verifies the effectiveness of its compliance measures).

102. *Proposed Regulation*, *supra* note 1, art. 22(2)(b), at 55 (including as an appropriate measure "implementing the data security requirements laid down in Article 30"). *See also id.*, art. 30(1), at 60 ("The controller and the processor shall implement appropriate technical and

- The obligation to perform a data protection impact assessment in special circumstances;[103]

- The obligation to implement mechanisms to ensure the verification of the effectiveness of the measures described above.[104] This may require retaining an independent auditor to conduct the verification;[105] and

- The obligations of the data controller to ensure data protection by design and by default.[106]

3.4.2 Documentation Requirements: Supervision by Data Protection Authority

Article 28 details the obligation for controllers *and processors* to maintain documentation of the processing operations under their responsibility. This obligation would replace the current requirement to "notify" the local data protection supervisory authority, by providing a description of the company's data processing practices as required by the national laws that implement Articles 18 and 19 of Directive 95/46/EC.[107]

---

organisational measures to ensure a level of security appropriate to the risks represented by the processing and the nature of the personal data to be protected, having regard to the state of the art and the costs of their implementation.").

103. *Proposed Regulation*, *supra* note 1, art. 22(2)(c), at 55 (including as an appropriate measure "performing a data protection impact assessment pursuant to Article 33"). *See also id.*, art. 33, at 62-63 (requiring data impact assessments when processing operations present specific risks to data subjects by virtue of their "nature, their scope or their purposes," such as monitoring publicly accessible areas, use of the personal data of children, use of genetic data or biometric data, processing information on an individual's sex life, the use of information regarding health or race, or an evaluation having the effect of profiling or predicting behaviors).

104. *Proposed Regulation*, *supra* note 1, art. 22(3), at 55 ("The controller shall implement mechanisms to ensure the verification of the effectiveness of the measures referred to in paragraphs 1 and 2.").

105. *Id.* ("If proportionate, this verification shall be carried out by independent internal or external auditors.").

106. *Proposed Regulation*, *supra* note 1, art. 23(1)-(2), at 56 (requiring controllers, "both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organizational measures and procedures" to ensure compliance and data protection, and that by default, only personal data necessary for specific purposes are processed, and not retained beyond the minimum time necessary).

107. *See generally* GILBERT, *supra* note 3, *Chapter 13 "Austria," Chapter 14 "Belgium," Chapter 16 "Bulgaria,"Chapter 21 "Cyprus", Chapter 22 "Czech Republic," Chapter 23 "Denmark," Chapter 26 "Estonia," Chapter 27 "Finland," Chapter 28 "France," Chapter 29 "Germany," Chapter 30 "Greece," Chapter 32 "Hungary," Chapter 35 "Ireland," Chapter 37*

This removal of the notification requirement reflects one of the new guiding principles in the EU Data Protection reform: that of accountability.[108] Under the Proposed Regulation, data controllers and data processors must create their own structures and policies for the protection of personal data, and document them thoroughly.[109] They must be prepared to respond to any inquiry from their Data Protection Authority and to promptly produce these structures and policies.[110]

Article 28 identifies a long list of documents that would have to be created and maintained by data controllers *and data processors*.[111] The information required is somewhat similar to the information that is currently provided in notifications to the data protection authorities.[112] There are, however, new requirements such as the obligation to keep track of the transfers to third countries, or to keep track of the time limits for the erasure of the different categories of data.[113]

"Italy," Chapter 39 "Latvia," Chapter 41 "Lithuania," Chapter 42 "Luxembourg," Chapter 44 "Malta," Chapter 46 "The Netherlands," Chapter 49 "Poland," Chapter 50 "Portugal," Chapter 51 "Romania," Chapter 54 "Slovakia," Chapter 55 "Slovenia," Chapter 58 "Spain," Chapter 59 "Sweden," Chapter 64 "United Kingdom."

108. *See* Article 29 Data Protection Working Party, Opinion 3/2010 on the Principle of Accountability, 00062/10/EN/WP 173 (July 13, 2010), *available at* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp173_en.pdf.

109. *See Proposed Regulation*, *supra* note 1, arts. 22, 23 and 28, at 55-56, 58-59.

110. *Proposed Regulation*, *supra* note 1, art. 28(3), at 59 ("The controller and the processor . . . shall make the documentation available, on request, to the supervisory authority."); *id.*, art. 29, at 59 ("The controller and the processor . . . shall co-operate, on request, with the supervisory authority . . . by providing . . . information . . . and by granting access . . . . In response to the supervisory authority's exercise of its powers under Article 53(2), the controller and the processor shall reply to the supervisory authority within a reasonable period to be specified by the supervisory authority. The reply shall include a description of the measures taken and the results achieved, in response to the remarks of the supervisory authority.").

111. *Proposed Regulation*, *supra* note 1, arts. 28(2), at 58-59 (requiring documentation on the names and contact details of the controller and data protection officer (if any), purposes of the processing, categories of data subjects and the categories of personal data relating to them; the recipients or categories of recipients of the personal data, transfers of data to a third country, including any appropriate safeguards, time limits for erasure for the different categories of data, and the mechanisms by which the controller verifies the effectiveness of its compliance measures).

112. Council Directive 95/46/EC, *supra* note 9, art. 19(1)(a)-(f), 1995 O.J. (L 281) 44 (requiring: "(a) the name and address of the controller and of his representative, if any; (b) the purpose or purposes of the processing; (c) a description of the category or categories of data subject and of the data or categories of data relating to them; (d) the recipients or categories of recipient to whom the data might be disclosed; (e) proposed transfers of data to third countries; (f) a general description allowing a preliminary assessment to be made of the appropriateness of the measures taken pursuant to Article 17 to ensure security of processing.").

113. *Proposed Regulation*, *supra* note 1, arts. 28(2)(f)-(g), at 59 (requiring documentation "(f) where applicable, [on] transfers of data to a third country or an international organisation,

In the case of data controllers or data processors with operations in multiple countries, Article 51 would create the concept of the "main establishment." The Data Protection Supervisory Authority of the country where the data controller or data processor has its "main establishment" would be responsible for supervising the processing activities of that controller or processor in all Member States where the company or group of companies operates, subject to mutual assistance and cooperation provisions that are set forth in the Proposed Regulation.[114]

3.4.3 Allocation of Responsibilities among Joint Controllers

Articles 24 and 25 address some of the issues raised by outsourcing, offshoring and cloud computing. While these provisions do not clearly indicate whether or when outsourcers are joint data controllers, they acknowledge the fact that there may be more than one data controller.[115] Under Article 24, joint data controllers would be required to determine their own allocation of responsibility for compliance with the Proposed Regulation.[116] If they fail to do so, they would be held jointly responsible.[117] Article 25 would require data controllers that are not established in the European Union, to appoint a designated representative in the European Union, when their data

---

including the identification of that third country or international organisation and, in case of transfers referred to in point (h) of Article 44(1), the documentation of appropriate safeguards; (g) a general indication of the time limits for erasure of the different categories of data.").

114. *Proposed Regulation*, *supra* note 1, art. 51(2), at 77 ("Where the processing of personal data takes place in the context of the activities of an establishment of a controller or a processor in the Union, and the controller or processor is established in more than one Member State, the supervisory authority of the main establishment of the controller or processor shall be competent for the supervision of the processing activities of the controller or the processor in all Member States, without prejudice to the provisions of Chapter VII of this Regulation.").

115. *Proposed Regulation*, *supra* note 1, art. 24, at 56 ("Where a controller determines the purposes, conditions and means of the processing of personal data jointly with others, the joint controllers shall determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the procedures and mechanisms for exercising the rights of the data subject, by means of an arrangement between them.").

116. For an analysis of the circumstances under which a service provider (such as an outsourcer or cloud service provider) may be deemed a joint data controller, see Francoise Gilbert, *Cloud Service Providers Can Be Both Data Processors and Data Controllers*, BLOOMBERG BNA (Feb. 14, 2011), *available at*
http://my.bna.com/xpdt/display/batch_print_display.adp?searchid=18341086.

117. *Proposed Regulation*, *supra* note 1, art. 77(2), at 91 ("Where more than one controller or processor is involved in the processing, each controller or processor shall be jointly and severally liable for the entire amount of the damage.").

processing activities are subject to the Regulation.[118]

3.5 Data Protection Officer

Articles 35 through 37 would require data controllers *and data processors* to appoint a data protection officer. The rule would apply to the public sector, and, in the private sector, to enterprises employing more than 250 employees, or where the core activities of the controller or processor consist of processing operations that require regular and systematic monitoring of the data subjects.[119] Article 36 identifies the roles and responsibilities of the data protection officer and Article 37 defines the core tasks of the data protection officer.

Under the current data protection regime, several EU Member States, such as Germany, require organizations to appoint a Data Protection Officer who is responsible for the company's compliance with the national data protection law.[120] In the United States, numerous laws and FTC consent decrees also require entities to appoint a person to be responsible for all matters pertaining to data protection within the entity.[121]

3.6 Special Rules for Data Processors and Subcontractors

Article 27, which is based on Article 16 of Directive 95/46/EC, would generally follow the existing provisions to define the rules for processing under the authority of the data controller. As is currently

---

118. *Proposed Regulation*, *supra* note 1, art. 25, at 56-57 (requiring a controller "not established in the Union," involved in certain processing of personal data of data subjects residing in the Union, to appoint a representative established in one of the Member States where the data subjects reside).

119. *Proposed Regulation*, *supra* note 1, art. 35(1), at 65 ("The controller and the processor shall designate a data protection officer in any case where: (a) the processing is carried out by a public authority or body; or (b) the processing is carried out by an enterprise employing 250 persons or more; or (c) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects.").

120. *See, e.g.*, Bundesdatenschutzgesetz [BDSG, Federal Data Protection Act], Aug. 14, 2009, RGBl. I at § 4f, *available at*
http://www.bfdi.bund.de/EN/DataProtectionActs/Artikel/BDSG_idFv01092009.pdf?__blob=publicationFile.

121. *See, e.g.*, In the Matter of Google, Inc., Agreement Containing Consent Order, before the Federal Trade Commission, File No. 102 3136, *available at*
http://www.ftc.gov/os/caselist/1023136/110330googlebuzzagreeorder.pdf; In the Matter of Facebook Inc., Agreement Containing Consent Order, before the Federal Trade Commission, File No. 092 3184, *available at*
http://ftc.gov/os/caselist/0923184/120810facebookdo.pdf.

the case, data processors would be directly prohibited from processing personal data unless directed to do so by the data controller.[122]

Article 26 would build on Article 17(2) of Directive 95/46/EC and increase the obligations of the data processors.[123] It would add a very important element: a processor who processes data beyond the instructions provided by the controller would be considered a joint controller.[124] This very important clarification is consistent with Working Paper WP 169 issued by the Article 29 Working Party in February 2010.[125] In this paper, the Article 29 Working Party discussed when a data processor becomes a joint controller with the initial data controller.[126]

This clarification is likely to generate significant changes in the relations between a company and its service providers—such as outsourcers and cloud service providers. In numerous contracts, the service providers require the client to agree that the service provider retains the freedom to make many changes or to make decisions such as when or where to modify the application, to back up data, or to locate a disaster recovery site. On the other hand, most cloud service providers have insisted that the client agree to a contractual provision where the client acknowledges that the cloud service provider is a data processor and not a data controller.[127] If a cloud service provider

---

122. *Proposed Regulation*, *supra* note 1, art. 27, at 58 ("The processor and any person acting under the authority of the controller or of the processor who has access to personal data shall not process them except on instructions from the controller, unless required to do so by Union or Member State law.").

123. *See Proposed Regulation*, *supra* note 1, at 10 ("Article 26 clarifies the position and obligation of processors, partly based on Article 17(2) of Directive 95/46/EC, and adding new elements, including that a processor who processes data beyond the controller's instructions is to be considered as a joint controller."); *id.*, art. 26(1), at 57-58 (text of Article 26).

124. *Proposed Regulation*, *supra* note 1, art. 26(4), at 57 ("If a processor processes personal data other than as instructed by the controller, the processor shall be considered to be a controller in respect of that processing and shall be subject to the rules on joint controllers laid down in Article 24.").

125. Working Paper WP 169 issued by the Article 29 Working Party in February 2010. Article 29 Data Protection Working Party, Opinion 1/2010 on the Concepts of "controller" and "processor," 00264/10/EN/WP 169, 17-18 (Feb. 16. 2010), available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf (discussing when a data processor becomes a joint controller with the initial data controller).

126. *See also* Gilbert, *supra* note 116.

127. Article 29 Data Protection Working Party, Opinion 05/2012 on Cloud Computing, 01037/12/EN/WP 196, 8 (July 1, 2012), *available at* http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf. ("[C]lients of cloud computing services may not have room for manoeuvre in negotiating the contractual terms of use of the cloud services as standardised offers are a feature of many cloud computing services. Nevertheless, it is ultimately the client who decides on the allocation of part

chose to move a data center or disaster recovery center to a different location without consulting with the client, would it become a joint-controller if the provisions of this new Article 26 were applied? Probably yes.

3.7 Security of Personal Information

Articles 30 through 32 focus on the security of personal data.

3.7.1 Obligation to Provide Adequate Security

Article 30 of the Proposed Regulation builds on the security requirements already found in Article 17(1) of Directive 95/46/EC and extends these obligations to the data processors. Under Article 30, both the data controller *and data processor* would be required to implement appropriate security measures, irrespective of the terms of the contract. Among other things, this provision is likely to affect cloud computing agreements where the cloud service provider places the sole burden of providing adequate security on the client, and disclaims any liability for loss of the data.

3.7.2 Security Breach Disclosure

In addition, the Proposed Regulation introduces an obligation to provide notification of "personal data breaches."[128] The term "personal data breach" is defined as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed."[129]

In case of a breach of security, a data controller would be required to inform the supervisory authority within 24 hours, if feasible.[130] A data processor that is the victim of a breach would also be required to alert and inform the data controller immediately after establishing that a breach of security occurred.[131]

---

or the totality of processing operations to cloud services for specific purposes; the cloud provider's role will be that of a contractor vis-à-vis the client . . . .").

128. *Proposed Regulation*, *supra* note 1, at 10 ("Articles 31 and 32 introduce an obligation to notify personal data breaches, building on the personal data breach notification in Article 4(3) of the e-privacy Directive 2002/58/EC.").

129. *Proposed Regulation*, *supra* note 1, art. 4(9), at 42.

130. *Proposed Regulation*, *supra* note 1, art. 31(1), at 60 ("In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 24 hours after having become aware of it, notify the personal data breach to the supervisory authority.").

131. *Proposed Regulation*, *supra* note 1, art. 31(2), at 60 ("Pursuant to point (f) of Article 26(2), the processor shall alert and inform the controller immediately after the establishment of a

If the breach is "likely to adversely affect the protection of the personal data or the privacy of the data subject," the data controller is required to notify the data subjects, without undue delay, after it has notified the supervisory authority of the breach.[132] According to the preamble, a breach is "likely to affect the protection" of personal data if it could result in identity theft, fraud, physical harm, significant humiliation or damage to reputation.[133]

3.8 Additional Requirements

3.8.1 Data Protection Impact Assessment

While the Proposed Regulation would relax some of the administrative burden, such as the notification requirements,[134] it would contain stricter obligations with respect to certain categories of processing that represent special risks. A data protection impact assessment would be required, and a prior consultation with, and authorization from, the data protection authority would be needed.[135]

Article 33 would require controllers *and processors* to carry out a data protection impact assessment if the proposed processing is likely to present specific risks to the rights and freedoms of the data subjects by virtue of its nature, scope, or purposes. Examples of these activities include: monitoring publicly accessible areas, use of the personal data of children, use of genetic data or biometric data, processing information on an individual's sex life, the use of information regarding health or race, or an evaluation having the effect of profiling or predicting behaviors.[136]

---

personal data breach.").

132. *Proposed Regulation*, *supra* note 1, art. 32(1), at 61.

133. *Proposed Regulation*, *supra* note 1, at 28 (Preamble paragraph 67 states "A breach should be considered as adversely affecting the personal data or privacy of a data subject where it could result in, for example, identity theft or fraud, physical harm, significant humiliation or damage to reputation.").

134. *See* Council Directive 95/46/EC, *supra* note 9, arts. 18-21, 1995 O.J. (L 281) 43-44 (EC).

135. *Proposed Regulation*, *supra* note 1, art. 33(1), at 62 ("Where processing operations present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes, the controller or the processor acting on the controller's behalf shall carry out an assessment of the impact of the envisaged processing operations on the protection of personal data."). *See also id.*, art. 34(2), at 63-64.

136. *Proposed Regulation*, *supra* note 1, art. 33(2)(a)-(d), at 62-63.

3.8.2 Consultation and Authorization

Article 34 would set forth the requirement for consulting with the data protection authority and obtaining its prior authorization in the case of certain categories of processing that present special risks. This provision is built on Article 20 of Directive 95/46/EC.

3.9 Rights of the Data Subjects

Articles 11 through 20 would define the rights of the data subjects. The Proposed Regulation would increase the rights of data subjects, and improve their ability to have access to, and control over, their personal information.[137] In addition to the right of information, right of access, and right of rectification, which exist in the current regime, the Proposed Regulation introduces the "right to be forgotten" as part of the right to erasure, and the "right to data portability."[138]

3.9.1 Transparency and Better Communications

Article 11 of the proposed Regulation would introduce the obligation for data controllers to provide the data subjects with transparent and easily accessible and understandable information, while Article 12 would require them to provide procedures and a mechanism for the exercise of the data subject's rights. This would include identifying means for electronic requests, requiring that response to the data subject's request be made within a defined deadline, and identifying the motivation of refusals.

Companies will welcome the fact that the rules for handling requests for access or deletion would be the same in all Member States. In the current regime, the time frames for responding to such requests are different, with some Member States requiring action within very short periods of time, and others allowing up to two

---

137. *See, e.g.*, *Proposed Regulation*, *supra* note 1, art. 15(2), at 50 ("The data subject shall have the right to obtain from the controller communication of the personal data undergoing processing."), *id.*, arts. 16-19, at 51-53 (detailing, respectively, the data subject's rights to rectification, erasure, data portability and to object).

138. *Proposed Regulation*, *supra* note 1, art. 17, at 51 ("The data subject shall have the right to obtain from the controller the erasure of personal data relating to them and the abstention from further dissemination of such data, . . . where one of the following grounds applies: (a) the data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; (b) the data subject withdraws consent . . . or when the storage period consented to has expired, and where there is no other legal ground for the processing of the data; (c) the data subject objects to the processing of personal data pursuant to Article 19; (d) the processing of the data does not comply with this Regulation for other reasons.").

months for responding.[139]

Article 13 would provide rights for data subjects in relation to recipients. This provision is based on Article 12(c) of Directive 95/46/EC.[140] It would require the data controller to communicate any rectification or erasure carried in connection with the data subject's right to correction and blocking to each recipient to whom the data have been disclosed.[141] Like under Directive 95/46/EC, there would be a limit to this obligation when this communication would prove impossible or involve a disproportionate effort.[142] The notion of "recipient" includes all natural or legal persons, public authority, agency, or other body to whom the data would have been disclosed, including joint controllers and processors of the personal data.[143]

3.9.2 Right of Information

The right of information would be expanded beyond that which is defined in Articles 10 and 11 of Directive 95/46/EC,[144] to require that data subjects be provided with more information than is currently required. For example, individuals would have to be informed of the length of the period during which the data controller intends to hold

---

139. *See, e.g.*, *Access to personal data*, INFORMATION COMMISSIONER'S OFFICE, UNITED KINGDOM, http://www.ico.gov.uk/for_organisations/data_protection/the_guide/principle_6/access_to_personal_data.aspx (last visited Aug. 11, 2012) (UK's Data Protection Act provides 40 days for responding); Commission Nationale de l'Informatique et des Libertés (CNIL), Decree No 2005-1309 of 20 October 2005 Enacted for the Application of Act No 78-17 of 6 January 1978 on Data Processing, Files and Individual Liberties, art. 94, *available at* http://www.cnil.fr/fileadmin/documents/en/Decree%202005-1309.pdf (In France, responses to data subject access requests must be given within two months.).

140. Council Directive 95/46/EC, *supra* note 9, art. 12(c), 1995 O.J. (L 281) 42 (stating "Member States shall guarantee every data subject the right to obtain from the controller: . . . (c) notification to third parties to whom the data have been disclosed of any rectification, erasure or blocking carried out in compliance with (b), unless this proves impossible or involves a disproportionate effort.").

141. *Proposed Regulation*, *supra* note 1, art. 13, at 48 ("The controller shall communicate any rectification or erasure carried out in accordance with Articles 16 and 17 to each recipient to whom the data have been disclosed, unless this proves impossible or involves a disproportionate effort.").

142. *Id.*

143. *Proposed Regulation*, *supra* note 1, art. 4(7), at 42 ("'recipient' means a natural or legal person, public authority, agency or any other body to which the personal data are disclosed;"); *id.* at 8 ("Article 13 provides rights in relation to recipients, based on Article 12(c) of Directive 95/46/EC, extended to all recipients, including joint controllers and processors.").

144. Council Directive 95/46/EC, *supra* note 9, arts.10-11, 1995 O.J. (L 281) 41-42 (specifying information to be given to the data subject whether data obtained from the data subject or from third parties).

their data.[145] They would also have to be informed of their right to lodge a complaint, of the proposed cross-border transfers of personal data, and of the source from which the data are originating.[146]

3.9.3 Right of Access

The right of access to personal data, which is already found in Article 12(a) of Directive 95/46/EC, would contain additional elements, such as the obligation to inform the individuals of the storage period, of their rights to erasure and rectification, as well as their right to lodge a complaint.[147]

3.9.4 Right of Rectification

Article 16 of the Proposed Regulation would retain the right of rectification, which was defined in Article 12(b) of Directive 95/46/EC.[148]

3.9.5 Right to Object to the Processing

Article 14 of Directive 95/46/EC contained a right to object to the processing of personal data. This right would be provided by Article 19 of the Proposed Regulation, but the burden of proof would switch to the data controller, while it is currently on the data subject.[149]

Under the new Article 19, the data subjects would have the right to object at any time to the processing of personal data that has been made without their consent allegedly for (i) the protection of their vital interests or (ii) the performance of a task carried out in the public

---

145. *Proposed Regulation*, *supra* note 1, art. 14(1)(c), at 48 ("Where personal data relating to a data subject are collected, the controller shall provide the data subject with at least the following information: . . . (c) the period for which the personal data will be stored;").

146. *Proposed Regulation*, *supra* note 1, art. 14(1)(e) and (g), at 48-49 ("Where personal data relating to a data subject are collected, the controller shall provide the data subject with at least the following information: . . . (e) the right to lodge a complaint to the supervisory authority and the contact details of the supervisory authority; . . . (g) where applicable, that the controller intends to transfer to a third country or international organisation and on the level of protection afforded by that third country or international organisation by reference to an adequacy decision by the Commission;"); *id.*, art. 14(3), at 49 ("Where the personal data are not collected from the data subject, the controller shall inform the data subject, in addition to the information referred to in paragraph 1, from which source the personal data originate.").

147. *Proposed Regulation*, *supra* note 1, at 9 ("Article 15 provides the data subject's right of access to their personal data, building on Article 12(a) of Directive 95/46/EC and adding new elements, such as to inform the data subjects of the storage period, and of the rights to rectification and to erasure and to lodge a complaint."); *id.*, art. 15, at 50-51.

148. *Proposed Regulation*, *supra* note 1, at 9.

149. *Id.*; Council Directive 95/46/EC, *supra* note 9, art. 14(a), 1995 O.J. (L 281) 42-43.

interest or in the exercise of official authority vested in the controller, or (iii) the legitimate interests of the controller.[150] The controller would have to demonstrate that there are compelling legitimate grounds for the processing that override the interests or fundamental rights and freedoms of the data subject.[151] Under Article 14(a) of Directive 95/46/EC, the burden is on the data subject.[152] A data subject who wants to object to the processing of his personal data must show that there are compelling legitimate grounds relating his particular situation, to object to the processing of the data relating to him.[153]

The new Article 19 would also change the current Article 14(b), which allows data subject to object to the use of their personal data for marketing purposes. Under the Proposed Regulation, in addition to providing data subject to this right, companies would have to do so "in an intelligible manner" and the disclosure would have to be "clearly distinguishable from other information."[154] This is consistent with the general tone of the Proposed Regulation, which requires more transparency and more accountability from data holders. It is not clear, however, how this new provision would interact with the provisions in Directive 2002/58/EC, which regulates the use of unsolicited commercial messages. The 2002 Directive provides more specific and detailed requirements for companies to be allowed to send commercial messages to individuals, including a dual concept of opt-in and opt-out.[155] The Proposed Regulation appears to ignore the additional clarifications and nuances that were introduced by Directive 2002/58/EC.

3.9.6 Right not to be Subject to Measures Based on Profiling

Article 20 would provide data subjects with a right not to be subject to measures based on profiling. The provision generally

---

150. *Id.* at 53.

151. *Id.*

152. Council Directive 95/46/EC, *supra* note 9, art. 14(a), 1995 O.J. (L 281) 42-43 ("Member states shall grant data subjects the right . . . to object at any time on compelling legitimate grounds relating to his particular situation, save where otherwise provided by national legislation. Where there is a justified objection, the processing instigated by the controller may no longer involve that data.").

153. *Id.*

154. *Proposed Regulation*, *supra* note 1, at 53.

155. Council Directive, 2002/58/EC, para (40), 2002 O.J. (L 201/37) 41 (EC), *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0047:en:PDF.

follows the provisions currently in Article 15(1) of Directive 95/46/EC, and enhances them with modifications and additional safeguards.[156]

3.9.7 Right to be Forgotten and Right to Erasure

The right to erasure, originally in Article 12(b) of Directive 95/46/EC, would be significantly strengthened. In the current regime, individuals may obtain the erasure of their data only in limited circumstances.[157] Article 17 of the Proposed Regulation would provide the conditions for the exercise of the "right to be forgotten." Data subjects would have the right to obtain from the data controller the "erasure of personal data relating to them and the abstention from further dissemination of such data" in specific circumstances.[158] In addition, the data controller who has made the personal data public would have to inform third parties of the data subject's request to erase any links to the personal data and any copy or replication of the personal data.[159]

It is not clear how this provision would be implemented in practice. Numerous companies and scholars have commented on the practical aspects of the implementation as well as the consequences, such as a threat to free speech.[160]

3.9.8 Right to Data Portability

Article 18 would introduce the data subject's right to "data portability", that is, the right to transfer data from one automated processing system to another, without being prevented from doing so by the data controller. This right would include the right to obtain

---

156. *Proposed Regulation*, *supra* note 1, at 9.

157. Council Directive 95/46/EC, *supra* note 9, art. 12(b), 1995 O.J. (L 281) 42 ("Member States shall guarantee every data subject the right to obtain from the controller: . . . (b) as appropriate the rectification, erasure, or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data.").

158. *Proposed Regulation*, *supra* note 1, art. 17(1), at 51 ("The data subject shall have the right to obtain from the controller the erasure of personal data relating to them and the abstention from further dissemination of such data," under any of four enumerated grounds.).

159. *Proposed Regulation*, *supra* note 1, art. 17(2), at 51 ("Where the controller referred to in paragraph 1 has made the personal data public, it shall take all reasonable steps, including technical measures, in relation to data for the publication of which the controller is responsible, to inform third parties which are processing such data, that a data subject requests them to erase any links to, or copy or replication of that personal data.").

160. *See e.g.*, Jeffrey Rosen, *The Right to Be Forgotten*, 64 STAN. L. REV. ONLINE 88 (2012), *available at* www.stanfordlawreview.org/online/privacy-paradox/right-to-be-forgotten.

one's data from the controller in a structured and commonly used electronic format.[161] The Regulation is technology neutral. It does not explain how the copy could be created and what format can be used to ensure that the file can be uploaded and read by a different social media platform.

The "right to be forgotten" and the "right to portability" reflect the pressure of the current times. There have been numerous reports of the unexpected consequence of the use of social media.[162]

Social network users discovered that these free and simple services came at a price, their personal data.[163] More specifically that their personal data could be used in forms that they had not contemplated, would be shared with, or disclosed to, others, and that the service provider would resist a user's attempt to move to another service.[164]

From a company's perspective it is not clear how and to what extent the right to be forgotten and the right to portability could be implemented. The right to be forgotten poses significant practical problems. Once data, statements, photographs, have been published on the Internet, they can be quickly disseminated, copied, integrated in other content or databases. The social network or other service that

---

161. *Proposed Regulation*, *supra* note 1, art. 18(1), at 53 ("The data subject shall have the right, where personal data are processed by electronic means and in a structured and commonly used format, to obtain from the controller a copy of data undergoing processing in an electronic and structured format which is commonly used and allows for further use by the data subject.").

162. *See, e.g.*, Bernhard Debatin et al., *Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences*, 15 J. COMPUTER-MEDIATED COMM. 83 (2009), *available at* http://onlinelibrary.wiley.com/doi/10.1111/j.1083-6101.2009.01494.x/pdf; Riva Richmond, *Can you Protect Your Image While on Facebook?*, N.Y. TIMES GADGETWISE BLOG (July 24, 2009), *available at* http://gadgetwise.blogs.nytimes.com/2009/07/24/can-you-protect-your-image-while-on-facebook/; Jeffrey Rosen, *The Web Means the End of Forgetting*, N.Y. TIMES, July 21, 2010, at MM30, *available at*
https://www.nytimes.com/2010/07/25/magazine/25privacy-t2.html?_r=1&ref=magazine&pagewanted=all; Minda Zetlin, *Unintended Consequences: How to Keep Social Media from Becoming a Security Risk*, INC., (Jan. 11, 2011),
http://www.inc.com/internet/articles/201101/unintended-consequences-how-to-keep-social-media-from-becoming-a-security-risk.html.

163. *See, e.g.*, Kashmir Hill, *Max Schrems: The Austrian Thorn in Facebook's Side*, FORBES (Feb. 7, 2012), http://www.forbes.com/sites/kashmirhill/2012/02/07/the-austrian-thorn-in-facebooks-side/.

164. *See, e.g.*, Scott Thurm and Yukari Iwatani Kane, *Your Apps are Watching You*,WALL ST. J., (Dec. 17, 2010),
http://online.wsj.com/article/SB10001424052748704694004576020083703574602.html
(finding through a detailed investigation that free apps such as Angry Birds, Pandora and the New York Times collected user location information without permission, and transmitted that information to third parties).

initially served as the publisher of the items in question would have no way to know who copied or republished that item, and would have no ability to identify these third parties or to exercise control over these third parties. Data may also be stored in archives or on back up media, or duplicated on a host site for disaster recovery and business continuity purposes. On the other hand, content that was intentionally provided to subcontractors, service providers or co-marketers might be more easily traceable in some circumstances, for example, if the company keeps a log of its data transfers.

3.10 Complaints, Judicial Remedies, Class Actions

Articles 73 through 79 would address remedies, liability, and sanctions. While some provisions build on the current framework set forth in Directive 95/46/EC, some new provisions would significantly increase companies' exposure to complaints, enforcement, and legal expenses.

3.10.1 Right to Lodge a Complaint with a Supervisory Authority

Article 73 would grant data subjects the right to lodge a complaint with a supervisory authority. This right is similar to the right under Article 28 of Directive 95/46/EC.

3.10.2 Judicial Remedy against Data Controllers or Processors

In addition to the administrative remedies described above, individuals would have a private right of action against a data controller *or a data processor*. Article 75 would grant individuals the right to seek a judicial remedy against a controller or processor. The concept is similar to that which is provided in Article 22 of Directive 95/46/EC. The new clause indicates clearly that action may be filed against the data controller or data processor and would provide individuals with a choice of courts. The action could be brought in a court of the Member State where the defendant is established or where the data subject is residing.

3.10.3 Judicial Remedy against Supervisory Authorities

Article 74 would provide a judicial remedy against a decision of a supervisory authority, similar to that which is found in Article 28(3) of Directive 95/46/EC. This remedy would oblige a data protection

authority to act on a complaint.[165] The courts of the Member State where the data protection authority is located would be competent to hear the matter.[166] In addition, it would allow the data protection authority of the Member State where an individual resides to bring proceedings on behalf of a data subject before the courts of another Member State where the competent (but delinquent) data protection authority is established in order to require that it take action.[167]

3.10.4 Class Actions

Articles 73 and 76 of the Proposed Regulation increase the number of entities that can file a complaint. In addition to individuals, consumer organizations and similar associations would have the right to lodge complaints on behalf of a data subject or, in case of a personal data breach, on their own behalf.[168] In addition, Article 76 would grant bodies, organizations and associations, such as consumer associations or other organizations that aim to protect privacy rights, the right to seek judicial remedies against data controllers *or data processors* that have infringed their members' rights in violation of the Regulation, or against a decision of a supervisory authority concerning their members.

These additions are very important. They would open the door to actions similar to a class action suit, a form of action that is currently seldom used in the European Union, but with which U.S. companies

---

165. *Proposed Regulation*, *supra* note 1, art. 74(2), at 90 ("Each data subject shall have the right to a judicial remedy obliging the supervisory authority to act on a complaint in the absence of a decision necessary to protect their rights, or where the supervisory authority does not inform the data subject within three months on the progress or outcome of the complaint pursuant to point (b) of Article 52(1).").

166. *Proposed Regulation*, *supra* note 1, art. 74(3), at 90 ("Proceedings against a supervisory authority shall be brought before the courts of the Member State where the supervisory authority is established.").

167. *Proposed Regulation*, *supra* note 1, art. 74(4), at 90 ("A data subject which is concerned by a decision of a supervisory authority in another Member State than where the data subject has its habitual residence, may request the supervisory authority of the Member State where it has its habitual residence to bring proceedings on its behalf against the competent supervisory authority in the other Member State.").

168. *Proposed Regulation*, *supra* note 1, art. 73(2), at 89 ("Any body, organisation or association which aims to protect data subjects' rights and interests concerning the protection of their personal data . . . shall have the right to lodge a complaint with a supervisory authority in any Member State on behalf of one or more data subjects if it considers that a data subject's rights under this Regulation have been infringed as a result of the processing of personal data."); *id.*, art. 73(3), at 90 ("Independently of a data subject's complaint, any body, organisation or association referred to in paragraph 2 shall have the right to lodge a complaint with a supervisory authority in any Member State, if it considers that a personal data breach has occurred.").

are familiar. Many of the class actions currently filed in the United States are quite expensive for companies, and frequently bring little relief to the actual injured parties or the named plaintiffs.[169] Damages, if any, awarded against a company frequently consist in the payment of funds that benefit research institutions, non-profit privacy advocates or consumer organizations and the payment of the plaintiff's attorneys fees. The injured parties or the parties directly affected by an incident may only receive a very small amount of money compared to the large settlement amount. However even if the individuals on behalf of whom the lawsuit was filed might receive only a minimal compensation for the damages—tangible or not—that they incurred, the defendant in the suit will have incurred significant cost and expenses in defending the class action suit.

3.11 Damages and Sanctions

The proposed Regulation would significantly increase the stakes in case of unlawful processing or violation of applicable provisions. Articles 77 to 79 provide for right to compensation for the individuals, and penalties and administrative sanctions against data controllers *and data processors*.

3.11.1 Individuals' Right to Compensation

The individual's right to compensation is set out in Article 77 of the proposed Regulation. Under the new rule, individuals would be entitled to receive damages from data controllers, data processors, joint controllers, and joint processors, for the damages suffered.[170] When more than one entity is involved in the processing, the controllers *and processors* would be held jointly and severally liable for the entire amount of the damages.[171] There is no similar provision in Directive 95/46/EC.

3.11.2 Penalties and Sanctions

Articles 78 and 79 address penalties and sanctions. According to

---

169. *See, e.g.*, Leslie Wright, *Plaintiffs Won at Their Expense*, THE BURLINGTON FREE PRESS, May 22, 2003.

170. *Proposed Regulation*, *supra* note 1, art. 77(1), at 91 ("Any person who has suffered damage as a result of an unlawful processing operation or of an action incompatible with this Regulation shall have the right to receive compensation from the controller or the processor for the damage suffered.").

171. *Proposed Regulation*, *supra* note 1, art. 77(2), at 91 ("Where more than one controller or processor is involved in the processing, each controller or processor shall be jointly and severally liable for the entire amount of the damage.").

the Proposed Regulation, these penalties would have to be "effective, proportionate and dissuasive."[172]

Article 78 would require Member States to lay down rules on penalties and to report to the Commission on the provisions that it will have adopted. Article 78(1) would require Member States to take all measures necessary to ensure that the penalties are implemented, including where the controller did not comply with the obligation to designate a representative. In addition, Article 78(2) would require that, if the data controller has established a representative, any penalties be applied to the representative, without prejudice to any penalties which could be initiated against the controller.

Article 79 would grant each data protection authority the power to impose administrative sanctions. The criteria to be used in determining the amount of the administrative would include:

- Nature, gravity, and duration of the violation;
- Intentional or negligent character of the infringement;
- Degree of responsibility of the natural or legal person;
- Previous breaches of the law;
- Technical, organizational and administrative measures implemented to protect the security of personal information; and
- Degree of cooperation with the supervisory authority in order to remedy the violation, infringement, or breach of the law.[173]

The Proposed Regulation introduces significant sanctions for

---

172. *Proposed Regulation*, *supra* note 1, art. 78(1), at 91-92 ("The penalties provided for must be effective, proportionate and dissuasive."); *id.*, art. 79(2), at 92 ("The administrative sanction shall be in each individual case effective, proportionate and dissuasive.").

173. *Proposed Regulation*, *supra* note 1, art. 79(2), at 92 ("The amount of the administrative fine shall be fixed with due regard to the nature, gravity and duration of the breach, the intentional or negligent character of the infringement, the degree of responsibility of the natural or legal person and of previous breaches by this person, the technical and organizational measures and procedures implemented pursuant to Article 23 and the degree of cooperation with the supervisory authority in order to remedy the breach.").

violation of the law. Organizations would be exposed to penalties of up to 1 million Euros or up to 2% of the *global* annual turnover of an enterprise.[174] This is much more than the penalties currently in place throughout the European Union.[175] The Proposed Regulation signals an intent to more aggressively pursue the infringers and to equip the enforcement agencies with substantial tools to ensure compliance with the law.

There would be three categories of fines applicable to specific categories of violations.

- Fines up to 250,000 Euros or .5% of the annual *worldwide* turnover of an enterprise for minor violations; such as failure to provide proper mechanisms for the exercise of the right of access; or charging a fee to provide information.[176]

- Fines up to 500,000 Euros or 1% of the annual *worldwide* turnover of an enterprise for most violations, such as: failure to provide access or information; failure to maintain required documentation; failure to comply with the right to be forgotten.[177]

---

174. *Proposed Regulation*, *supra* note 1, art. 79(6), at 93.

175. Current EU penalties are far less than those proposed by the new regulation. For example in the UK for serious breaches, the penalty was recently raised to 500,000 GBP (before 2010, the penalty was 5,000 GBP). ALFRED BÜLLESBACH, CONCISE EUROPEAN IT LAW 110 (2010). In Germany, fines may reach up to 300,000 EUR plus any profits obtained as a part of the wrongdoing. *Id.* However, most penalties that have been assessed against companies are actually much less. For example, France recently assessed a 100,000 EUR penalty against Google. *Google Street View: CNIL pronounces a fine of 100,000 Euros*, COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS (CNIL) (Mar. 21, 2011), http://www.cnil.fr/english/news-and-events/news/article/google-street-view-cnil-pronounces-a-fine-of-100000-euros. There are some exceptions, for example, in Spain, some penalties have exceeded the 600,000 EUR mark. *See* ALFRED BÜLLESBACH, CONCISE EUROPEAN IT LAW 110 (2010).

176. *Proposed Regulation*, *supra* note 1, art. 79(4), at 92 ("The supervisory authority shall impose a fine up to 250 000 EUR, or in case of an enterprise up to 0,5 % of its annual worldwide turnover, to anyone who, intentionally or negligently: (a) does not provide the mechanisms for requests by data subjects or does not respond promptly or not in the required format to data subjects pursuant to Articles 12(1) and (2); (b) charges a fee for the information or for responses to the requests of data subjects in violation of Article 12(4).").

177. *Proposed Regulation*, *supra* note 1, art. 79(5), at 92-93 ("The supervisory authority shall impose a fine up to 500 000 EUR, or in case of an enterprise up to 1 % of its annual worldwide turnover, to anyone who, intentionally or negligently: (a) does not provide the information, or does provide incomplete information, or does not provide the information in a sufficiently transparent manner, to the data subject pursuant to Article 11, Article 12(3) and Article 14; (b) does not provide access for the data subject or does not rectify personal data pursuant to Articles 15 and 16 or does not communicate the relevant information to a recipient

- Fines up to 1,000,000 Euros or 2% of the annual *worldwide* turnover of an enterprise for the most serious or egregious violations such as: processing personal data without a sufficient legal basis or failure to comply with the consent requirement; failure to adopt the required policies (such as a security policy); failure to notify of a breach of security; failure to comply with the restrictions on the cross border transfers of personal data.[178]

3.12 The Key Players

The Regulation would also make administrative changes, and formalize and streamline the way in which the administrative agencies have been operating. The Data Protection Authorities would subsist, and would receive additional powers. The Article 29 Working Party would have increased authority and a new name, better suited to its actual role.

3.12.1 Data Protection Supervisory Authorities

The Data Protection Supervisory Authorities would subsist as independent entities.[179] Their mission would be enlarged and they would be required to cooperate with each other.[180]

---

pursuant to Article 13; (c) does not comply with the right to be forgotten or to erasure, or fails to put mechanisms in place to ensure that the time limits are observed or does not take all necessary steps to inform third parties that a data subjects requests to erase any links to, or copy or replication of the personal data pursuant Article 17; . . . (f) does not or not sufficiently maintain the documentation pursuant to Article 28, Article 31(4), and Article 44(3); . . . .").

178. *Proposed Regulation*, *supra* note 1, art. 79(6), at 93-94 ("The supervisory authority shall impose a fine up to 1 000 000 EUR or, in case of an enterprise up to 2 % of its annual worldwide turnover, to anyone who, intentionally or negligently: (a) processes personal data without any or sufficient legal basis for the processing or does not comply with the conditions for consent pursuant to Articles 6, 7 and 8; . . . (e) does not adopt internal policies or does not implement appropriate measures for ensuring and demonstrating compliance pursuant to Articles 22, 23 and 30; . . . (h) does not alert on or notify a personal data breach or does not timely or completely notify the data breach to the supervisory authority or to the data subject pursuant to Articles 31 and 32; . . . (l) carries out or instructs a data transfer to a third country or an international organisation that is not allowed by an adequacy decision or by appropriate safeguards or by a derogation pursuant to Articles 40 to 44; . . . .").

179. *Proposed Regulation*, *supra* note 1, art. 47(1), (2), at 75 ("The supervisory authority shall act with complete independence in exercising the duties and powers entrusted to it. . . . The members of the supervisory authority shall, in the performance of their duties, neither seek nor take instructions from anybody.").

180. *Proposed Regulation*, *supra* note 1, at 12 ("Article 46 obliges Member States to establish supervisory authorities, based on Article 28(1) of Directive 95/46/EC and enlarging the mission of the supervisory authorities to co-operation with each other and with the

3.12.1.1 General Rules of Operation

Articles 46 to 54 would define the new rules of operation of the Data Protection Supervisory Authorities (DPA). While the provisions would build on the general principles of Article 28 of Directive 95/46/EC, the new rules would enlarge the data protection authority's mission and require them to cooperate with each other and with the European Commission[181] when implementing the relevant case law.[182]

Article 49 would grant each of the Member States the freedom to establish their data protection supervisory authority within the guidelines provided by the Regulation. This may result in inconsistency in the way the data protection authorities are governed and managed. For example, the Member States would have the freedom to determine the qualifications required for the appointments of the members of the data protection authorities, and the regulations governing the duties of the members and staff of the data protection authority.[183]

Article 51 would set out the competence of the data protection authorities while Article 52 and 54 would define their duties and Article 53 their powers. The competence of each data protection authority would be limited to its own national territory in most cases.[184] However, in the case of data processors or data controllers

---

Commission."); *id.*, art. 46(1), at 75 ("Each Member State shall provide that one or more public authorities are responsible for monitoring the application of this Regulation and for contributing to its consistent application throughout the Union, in order to protect the fundamental rights and freedoms of natural persons in relation to the processing of their personal data and to facilitate the free flow of personal data within the Union. For these purposes, the supervisory authorities shall co-operate with each other and the Commission.").

181. *Proposed Regulation*, *supra* note 1, at 12 ("Article 46 obliges Member States to establish supervisory authorities, based on Article 28(1) of Directive 95/46/EC and enlarging the mission of the supervisory authorities to co-operation with each other and with the Commission.").

182. *Proposed Regulation*, *supra* note 1, at 12 ("Article 47 clarifies the conditions for the independence of supervisory authorities, implementing case law by the Court of Justice of the European Union, inspired also by Article 44 of Regulation (EC) No 45/2001. Article 48 provides general conditions for the members of the supervisory authority, implementing the relevant case law and inspired also by Article 42(2) to (6) of Regulation (EC) 45/2001.").

183. *Proposed Regulation*, *supra* note 1, art. 49, at 76-77 ("Each Member State shall provide by law within the limits of this Regulation: . . . (b) the qualifications, experience and skills required to perform the duties of the members of the supervisory authority; . . . (f) the regulations and common conditions governing the duties of the members and staff of the supervisory authority; . . . .").

184. *Proposed Regulation*, *supra* note 1, art. 51(1), at 77 ("Each supervisory authority shall exercise, on the territory of its own Member State, the powers conferred on it in accordance with this Regulation.").

established in several countries, the data protection authority of the principal establishment of the corporate group would acquire a new competence as the lead authority for that corporate group.[185]

As this is currently the case, the duties of the data protection authorities would include hearing and investigation of complaints, raising public awareness of the rules, safeguards and rights,[186] and preparing annual reports.[187] The proposed powers of the data protection authority would be very similar to those that are set forth in Article 28(3) of Directive 95/46/EC and Regulation (EC) 45/2001, with some additional powers, such as the power to sanction administrative offenses.[188]

3.12.1.2 Cooperation and Consistency

The Proposed Regulation sets forth a series of rules that may help ensure cooperation and consistency among the data protection authorities. Articles 55 and 56 would introduce rules on mandatory mutual assistance and rules on joint operations. Article 57 would introduce a consistency mechanism for ensuring unity of application with respect to data processing that may concern data subjects in several Member States. In some cases, unity and consistency may be obtained through opinions of the European Data Protection Board,[189] discussed below. There are also provisions giving power to the

---

185. *Proposed Regulation*, *supra* note 1, art. 51(2), at 77 ("Where the processing of personal data takes place in the context of the activities of an establishment of a controller or a processor in the Union, and the controller or processor is established in more than one Member State, the supervisory authority of the main establishment of the controller or processor shall be competent for the supervision of the processing activities of the controller or the processor in all Member States, without prejudice to the provisions of Chapter VII of this Regulation.").

186. *Proposed Regulation*, *supra* note 1, art. 52(1), at 77-78 ("The supervisory authority shall: . . . (b) hear complaints lodged by any data subject, or by an association representing that data subject in accordance with Article 73, investigate . . . the matter . . . (d) conduct investigations either on its own initiative or on the basis of a complaint or on request of another supervisory authority . . . ."); *id.*, art. 52(2), at 78 ("Each supervisory authority shall promote the awareness of the public on risks, rules, safeguards and rights in relation to the processing of personal data.").

187. *Proposed Regulation*, *supra* note 1, art. 54, at 80 ("Each supervisory authority must draw up an annual report on its activities. The report shall be presented to the national parliament and shall be made be available to the public, the Commission and the European Data Protection Board.").

188. *Proposed Regulation*, *supra* note 1, at 13 ("Article 53 provides the powers of the supervisory authority, in parts building on Article 28(3) of Directive 95/46/EC and Article 47 of Regulation (EC) 45/2001, and adding some new elements, including the power to sanction administrative offences.").

189. *Proposed Regulation*, *supra* note 1, art. 58, at 82-83.

European Commission to intervene.[190]

3.12.2 European Data Protection Board

The "European Data Protection Board" would be the new name for the "Article 29 Working Party."[191] The new Board would consist of the European Data Protection Supervisor and the heads of the supervisory authority of each Member State.[192] The composition of the group would be slightly different from that of the Article 29 Working Party. The EU Commission would not be a member of the group.[193] However, the European Commission would have the right to participate in the activities and to be represented.[194]

Articles 65 and 66 clarify the independence of the European Data Protection Board and describe its expanded role and responsibilities. Article 68 sets out its decision-making procedures, which include the obligation to adopt rules of procedure. Article 71 sets out a Secretariat of the European Data Protection Board, a service provided by the European Data Protection Supervisor.

4. POSSIBLE DIVERGENCE AMONG THE MEMBER STATES?

Despite an obvious intent to ensure uniformity amongst the Member States, the Regulation contains numerous provisions that grant the Member States or their Data Protection Agencies the power to make decisions independently.

---

190. *Proposed Regulation*, *supra* note 1, art. 59(1), at 83-84 ("[T]he Commission may adopt, in order to ensure correct and consistent application of this Regulation, an opinion in relation to matters raised pursuant to Articles 58 or 61."). *See also id.*, art. 60(1), at 84 ("[T]he Commission may adopt a reasoned decision requiring the supervisory authority to suspend the adoption of the draft measure . . . where it appears necessary in order to . . . reconcile the diverging positions of the supervisory authority and the European Data Protection Board . . . ."); *id.*, art. 62(1), at 85 (authorizing the adoption of implementing acts by the Commission to "decid[e] on the correct application of this Regulation in accordance with its objectives and requirements").

191. *Proposed Regulation*, *supra* note 1, at 14 ("The European Data Protection Board replaces the Working Party on the Protection of Individuals with regard to the Processing of Personal Data set up under Article 29 of Directive 95/46/EC.").

192. *Proposed Regulation*, *supra* note 1, art. 64(2), at 86 ("The European Data Protection Board shall be composed of the head of one supervisory authority of each Member State and of the European Data Protection Supervisor.").

193. *Proposed Regulation*, *supra* note 1, at 14 ("It is clarified that the Commission is not a member of the European Data Protection Board, but has the right to participate in the activities and to be represented.").

194. *Proposed Regulation*, *supra* note 1, art. 64(4), at 86 ("The Commission shall have the right to participate in the activities and meetings of the European Data Protection Board and shall designate a representative.").

4.1 Ability to Create Additional Restrictions

Article 21 grants the Member States the power to restrict through legislative measures certain rights and obligations provided for in the Directive in order to safeguard, as necessary:

- Public security;
- The prevention, investigation, detection and prosecution of criminal offenses;
- Important economic or financial interests of the Member States or of the European Union, such as monetary, budgetary and taxation matters, and the protection of market stability and integrity;
- The prevention, investigation, detection of prosecutions of breaches of ethics for regulated professions;
- The monitoring, inspection or regulatory function connected with the above; or
- The protection of the data subjects or the rights and freedom of others.[195]

While this provision is substantially similar to Article 13 of Directive 95/46/EC, it should be expected that Member States might be tempted to use it in order to regain some of the freedoms that they may have lost otherwise as a result of the adoption of the Regulation.

The scope of this carve out is significant. It could drastically affect the hope for unity and consistency. Article 21 would allow Member States to make restrictions to the basic data protection principles that are set forth in:

- Article 5, which details the seven basic principles relating to the processing of personal data. For example: the obligation to process the data fairly and lawfully, and in a transparent manner, to collect only the minimum necessary,

195. *Proposed Regulation*, *supra* note 1, art. 21(1), at 54-55.

or to store the data only for as long as necessary;

- Articles 11 to 20, which define the basic rights of the data subjects. This includes the right to information, right of access, right of rectification, right of erasure, right to be forgotten, right to data portability, right to object, right not to be subject to a measure based on profiling; and

- Article 32, which would provide for an obligation of the data controller to notify the data subjects in case of a breach of security.

While this carve out may generally be consistent with the current Article 13 of Directive 95/46/EC, it might gain a new interest from Member States who would miss their past freedom and use it as a loophole to introduce or re-introduce their own provisions. Since January 25, 2012, we have heard several reports of critics made by Data Protection Authorities against the Regulation. For example, the French Data Protection Authority, CNIL, is opposing the Proposed Regulation because it says that the Regulation would largely deprive citizens of the protections offered by their national authorities.[196] The UK Data Protection Commissioner has also complained that the Proposed Regulation needed to be strengthened and that it would create compliance and enforcement problems.[197]

---

196. *Draft EU Regulation on Data Protection: The Defense of Data Protection Driven Apart from Citizens*, COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS (CNIL) (Jan. 31, 2012), http://www.cnil.fr/nc/en/la-cnil/actu-cnil/article/article/draft-eu-regulation-on-data-protection-the-defense-of-data-protection-driven-apart-from-citizens/ ("The CNIL is particularly concerned about the risk of an increased distance between European citizens and their national authorities. Indeed, by proposing that the competent authority is the one where the main establishment of a company is located, regardless the targeted public by its activity, national authorities are reduced to play a role of mailbox. . . . Such a reform will strengthen the bureaucratic and distant image of the European institutions and will deprive widely the citizens of the protection offered by their national authority."). *See also* Bloomberg BNA, *CNIL Opposes EC Data Regulation; Says Would Undercut National DPAs*, 11 PRIVACY & SECURITY LAW REPORT 3 (Jan. 30, 2012) ("France's data protection authority (CNIL) firmly opposes the European Commission's proposed data protection regulation because it would 'largely deprive citizens of protection offered by their national authorities,' it said in a Jan. 26 statement that is by far the most negative DPA public response to the proposal.").

197. Press Release, Information Commissioner's Office of the United Kingdom, Initial Response from the ICO on the European Commission's Proposal for a New General Data Protection Regulation (Jan. 25, 2012), *available at*

http://www.ico.gov.uk/news/latest_news/2012/statement-initial-response-new-data-protection-regulation-proposals-25012012.aspx ("Whilst recognising that there is inevitably some tension

With the door widely open by Article 21 to create amendments, restrictions and carve outs, it is likely that there will be divergence and inconsistency in the actual implementation and the interpretation of the document by the various Member States. The extent of these divergences is uncertain at this point.

4.2 Privacy and Freedom of Expression

In addition to the provisions of Article 21 of the Proposed Regulation, numerous other provisions could allow Member States to enact their own laws. For example, traditionally there has been an inconsistency between the right of privacy and the freedom of expression.[198] This discrepancy would subsist, and States would have the freedom to determine how privacy rights and freedom of information can coexist. Member States would have the authority to adopt exemptions and derogations from specific provisions of the Regulation where this is necessary to reconcile the right to the protection of personal data with the right of freedom of expression.[199]

The scope of the power of the Member States would nevertheless be somewhat restricted. The Member States would be required to report to the European Commission on the laws that they would have adopted.[200]

---

between the drive for harmonisation of data protection standards across the European Union and his desire for flexibility in focusing obligations on processing that poses genuine risks, the Commissioner believes that in a number of areas the proposal is unnecessarily and unhelpfully over prescriptive. This poses challenges for its practical application and risks developing a "tick box" approach to data protection compliance. The proposal also fails to properly recognise the reality of international transfers of personal data in today's globalised world and misses the opportunity to adjust the European regulatory approach accordingly.").

198. *See, e.g.*, Jeffrey Rosen, *The Right to be Forgotten*, 64 STANFORD L. REV. ONLINE 88, 88 (2012) ("Although [European Commissioner for Justice, Fundamental Rights, and Citizenship Viviane] Reding depicted the new right [to be forgotten] as a modest expansion of existing data privacy rights, in fact it represents the biggest threat to free speech on the Internet in the coming decade.").

199. *Proposed Regulation*, *supra* note 1, art. 80(1), at 94 ("Member States shall provide for exemptions or derogations from the provisions on the general principles in Chapter II, the rights of the data subject in Chapter III, on controller and processor in Chapter IV, on the transfer of personal data to third countries and international organisations in Chapter V, the independent supervisory authorities in Chapter VI and on co-operation and consistency in Chapter VII for the processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression in order to reconcile the right to the protection of personal data with the rules governing freedom of expression.").

200. *Proposed Regulation*, *supra* note 1, art. 80(2), at 95 ("Each Member State shall notify to the Commission those provisions of its law which it has adopted pursuant to paragraph 1 by the date specified in Article 91(2) at the latest and, without delay, any subsequent amendment law or amendment affecting them.").

4.3 Special Data Processing Situations

Articles 81, 82, 84, and 85 would also grant Member States special powers to enact their own laws in specific situations. This would be the case for the protection of health information,[201] the protection of employee personal data in the employment context,[202] rules regarding interaction with professionals having an obligation of secrecy[203] and the collection of personal data by churches and religious association.[204]

4.4 Operation of the Data Protection Supervisory Authorities

Divergences should be expected in the rules that pertain to the operations of the supervisory authorities. Articles 46 to 49 would grant each Member State the power to appoint one or several data protection authorities to be responsible for the monitoring of the application of the Regulation. Each Member State would have the

---

201. *Proposed Regulation*, *supra* note 1, art. 81(1), at 95 ("[P]rocessing of personal data concerning health must be on the basis of Union law or Member State law which shall provide for suitable and specific measures to safeguard the data subject's legitimate interests, and be necessary for: (a) the purposes of preventive or occupational medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional subject to the obligation of professional secrecy . . . or (b) reasons of public interest in the area of public health . . . or (c) other reasons of public interest in areas such as social protection, especially in order to ensure the quality and cost-effectiveness of the procedures used for settling claims for benefits and services in the health insurance system.").

202. *Proposed Regulation*, *supra* note 1, art. 82(1), at 95-96 ("Within the limits of this Regulation, Member States may adopt by law specific rules regulating the processing of employees' personal data in the employment context, in particular for the purposes of the recruitment, the performance of the contract of employment, including discharge of obligations laid down by law or by collective agreements, management, planning and organisation of work, health and safety at work, and for the purposes of the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment, and for the purpose of the termination of the employment relationship.").

203. *Proposed Regulation*, *supra* note 1, art. 84(1), at 96-97 ("Within the limits of this Regulation, Member States may adopt specific rules to set out the investigative powers by the supervisory authorities laid down in Article 53(2) in relation to controllers or processors that are subjects under national law or rules established by national competent bodies to an obligation of professional secrecy or other equivalent obligations of secrecy, where this is necessary and proportionate to reconcile the right of the protection of personal data with the obligation of secrecy. These rules shall only apply with regard to personal data which the controller or processor has received from or has obtained in an activity covered by this obligation of secrecy.").

204. *Proposed Regulation*, *supra* note 1, art. 85, at 97 (allowing an exemption for churches and religious associations or communities that apply "comprehensive rules relating to the protection of individuals with regard to the processing of personal data," provided such rules are brought in line with the Regulation, and that churches and religious associations establish an independent supervisory authority).

power to define the rules of operation of the data protection supervisory authority or authorities within its territory within the general rules set by the Regulation. Further, under Article 74, the Member States would be responsible for enforcing final court decisions against their local data protection supervisory authority.

4.5 Penalties

There may be differences, as well, with respect to the assessment of penalties. Article 78 would grant to the Member States the authority to lay down the rules on penalties applicable to infringements of the Regulation. Member States would also have the authority to take the measures necessary to implement these rules.

5. CONCLUSION

The terms of the Proposed Regulation are not a major surprise. For several months, Viviane Reding, Vice-President of the European Commission, and other representatives of the European Union have provided numerous descriptions of their vision for the new regime,[205] including through a draft of the documents published in December 2011,[206] which differs slightly from the January 25, 2012 version. It is

---

205. *See, e.g.*, *Safeguarding Privacy*, *supra* note 6, at 8-9 ("To enhance the Single Market dimension of data protection, the Commission proposes to: lay down data protection rules at EU level through a Regulation directly applicable in all Member States which will put an end to the cumulative and simultaneous application of different national data protection laws." (citations omitted)); Viviane Reding, Vice-President of the European Comm'n & European Union Justice Comm'r, Speech at the Aspen Institute's IDEA Project Conference: Privacy Standards in the Digital Economy: Enhancing Trust and Legal Certainty in Transatlantic Relations (Mar. 23, 2011) (transcript available at http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/11/210); Viviane Reding, Vice-President of the European Comm'n & European Union Justice Comm'r, Speech at the European Business Summit: The Reform of the EU Data Protection Directive: Impact on Businesses (May 18, 2011) (transcript available at http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/11/349&format=PDF&aged=1&language=EN&guiLanguage=en); Viviane Reding, Vice-President of the European Comm'n & European Union Justice Comm'r, Speech at the British Bankers Ass'n's Data Protection & Privacy Conference: Assuring Data Protection in the Age of the Internet (June 20, 2011) (transcript available at http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/11/452&format=PDF&aged=1&language=EN&guiLanguage=en); Viviane Reding, Vice-President of the European Comm'n & European Union Justice Comm'r, Remarks at the American Chamber of Commerce to the EU's Industry Coalition for Data Privacy: Building Trust in the Digital Single Market: Reforming the EU's Data Protection Rules (Nov. 28, 2011) (transcript available at http://ec.europa.eu/commission_2010-2014/reding/pdf/speeches/data-protection_en.pdf).

206. *See Proposed EU Data Protection Regulation—November 29, 2011 Draft*, IT LAW GROUP (Dec. 6, 2011), http://www.itlawgroup.com/resources/articles/229-proposed-data-

nevertheless exciting to see, at long last, the materialization of these descriptions, outlines, and wish lists.

Altogether, if the current provisions subsist in the final draft, the new Regulation will increase the rights of the individuals and the powers of the supervisory authorities. While the Regulation would create additional obligations and accountability requirements for organizations, the adoption of a single rule throughout the European Union will help simplify the information governance, procedures, record keeping, and other requirements for companies. That is unless the Member States take advantage of the numerous loopholes in the Proposed Regulation to reinstate the provision of their own laws that have been superseded by the Regulation.

Finally, it should also be remembered that Directive 95/46/EC has been a significant driving force in the adoption of data protection laws throughout the world. In addition to the 30 members of the European Economic Area, numerous other countries, such as Switzerland, Peru, Uruguay, Morocco, Tunisia, or the Dubai Emirate (in the Dubai International Financial District) have adopted data protection laws that follow closely the terms of Directive 95/46/EC.[207] It remains to be seen what effect the adoption of the Regulation will have on the data protection laws of these other countries.

---

protection-regulation-unveiled-by-eu-commission.html. ("The European Commission has just published drafts of the two documents that will form the new legal framework for the protection of personal data throughout the European Economic Area. The draft documents are intended to provide a last opportunity for comments.").

207. *See generally* GILBERT, *supra* note 3. In particular, Chapter 10A "Albania;" Chapter 10B "Andorra;" Chapter 11 "Argentina;" Chapter 25 "Dubai;" Chapter 35 "Isle of Man;" Chapter 45 "Mexico;" Chapter 45A "Monaco;" Chapter 45B "Morocco;" Chapter 52 "Russia;" Chapter 60 "Switzerland;" Chapter 62 "Tunisia;" and Chapter 66 "Uruguay".