# PROPOSED EU DATA PROTECTION REGULATION [*]

**Francoise Gilbert**

*Francoise Gilbert is the founder and Managing Director of the IT Law Group (www.itlawgroup.com), a niche law firm that focuses on US and global information privacy and security, data governance, cloud computing, big data and other emerging technology issues. She is the author of the two-volume treatise Global Privacy and Security Law, www.globalprivacybook.com (Aspen Publishers/Wolters Kluwer Law and Business), which analyzes the data protection laws of 68 countries across all countries. Ms. Gilbert can be reached at fgilbert@itlawgroup.com or at +1-650-804-1235.*

## § 6A.01 BACKGROUND

On January 25, 2012, the European Commission published a series of legislative texts that are intended to create a new data protection framework as part of a sweeping reform of the protection of personal data processed by private and public entities. The reform consists of:

- A draft Regulation setting out a general EU framework for data protection; and
- A draft Directive on protecting personal data processed for the purposes of prevention, detection, investigation or prosecution of criminal offences and related judicial activities.

The proposed *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* (Proposed Regulation)[1] is intended to supersede Directive 95/46/EC.

---



[*] The content of this chapter is based on the proposed General Data Protection Regulation as voted by the European Parliament, March 12 2014, and on the draft General Data Protection Regulation as published by the European Commission in January 2012.

[1] http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf.

The Proposed Regulation—as well as the proposed Directive—is currently being discussed by the two European Union co-legislators, the European Parliament and the Council of the EU in which national Ministers sit. To become law, the proposed text must be approved by these two co-legislators.

Since the initial introduction of the original text of the Proposed Regulation, much comment, lobbying, and controversies have taken place.

On March 12, 2014, the EU Parliament voted in favor of the Proposed Regulation (and the related Proposed Directive), while submitting a substantial number of amendments.[1.1]

Before delving into the detailed analysis of the provisions of the Proposed Regulation, 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.

[A] Historical Milestones

Since its creation, the European Union has 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. This was achieved by adopting directives and requiring the Member States to implement these directives in their national laws. When implementing the directives, each Member State, in fact, retained—or elected to take—a lot of independence and autonomy in using their own words to implement the directives in their national laws. While this strategy allowed establishing 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 their own personality—at times very different personalities and requirements. These inconsistencies and discrepancies created a difficult setting for companies operating in

[1.1] http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_dp_plenary_vote_140312_en.pdf; Jan Philipp Albrecht's Draft report, *available at* http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/pr/922/922387/922387en.pdf.

several Member States.

The ratification of the Treaty of Lisbon in late 2009 was a very important milestone in the morphing of the European Union as a united power.[2] It marked a critical step in the evolution of the Union, creating deep changes in its rules of operation, increasing the power of the European Commission and the European Parliament, removing the three-pillar system that fragmented the operations, and moving the federation into a closer, tighter structure. With the Treaty of Lisbon, the European Union moved toward more cohesion, more consistency, and more unity.

Shortly after the ratification of the Treaty of Lisbon, in November 2010, taking advantage of the new structure and new expanded powers, the European Commission announced its intent to reform the data protection regime in effect in the European Union and detailed its plans and goals in a lengthy document. The document, Communication (COM) 609,[3] outlined its plan to reform the data protection regime in the European Union to take advantage of the new structures created by the Treaty of Lisbon and to take into account the numerous major technological changes and cultural changes of the recent years.[4] 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 texts that were published in January 2012 and especially in the Proposed Regulation with respect to the protection of personal data with regard to the processing of personal data.

One of the concerns that were stressed in Communication 609 was the lack of harmony and consistency between the national data protection laws adopted by the 27 Member States. Communication 609 stressed that it was necessary to enhance the internal market dimension and there were significant divergences between the

---

[2]On the Treaty of Lisbon, see Chapter 4, "The Byzantine Process of European Data Protection Law Making"; *see also* http://www.consilium.europa.eu/treaty-of-lisbon?lang=en.

[3]*See* Chapter 5, § 5.05 "2010 Plan to Overhaul the Privacy Framework."

[4]http://www.itlawgroup.com/resources/articles/187-proposed-changes-to-the-eu-data-directives-what-consequences-for-businesses.html.

national data protection laws in a large number of sectors. These divergences were hampering the free flow of personal data and created legal uncertainties both for the individuals and for the custodians of personal data. The Commission stressed in particular that it intended to explore different possibilities for harmonization and simplification. It also indicated that it wished to provide the EU data subjects with the same level of protection regardless of the geographic location of the data controller.

Drafts of the proposed documents that would implement the concepts described in the Communication were published in January 2012. A period of consultation and comments followed. In late October 2013, the European Parliament Commission on Civil Liberties, Justice and Home Affairs (also known as the LIBE Committee), the Committee designated by the European Parliament to analyze the proposed text prepared under Viviane Reding, published a final Report (the LIBE Committee Report).

The LIBE Committee Report or "Report on the Proposal for a Regulation of the European Parliament and the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data (General Data Protection Regulation)" was drafted by Jan Philipp Albrecht, a Member of the European Parliament, in his role as Rapporteur for this project.

The LIBE Committee Report contains 196 proposed amendments to the recitals and the clauses of the January 2012 Proposed Draft Regulation. On March 12, 2014, the European Parliament voted to support the Proposed Regulation, which ensures that the project remains alive even after the Parliamentary elections of May 2014. The Parliament also strengthened some of the data protection amendments, in particular around the transfer of personal data to non-EU countries. It also backed a resolution calling for the suspension of the Safe Harbor Agreement with the United States. The vote gives a mandate to its Rapporteurs, MEP Albrecht and Droutsas, to enter into negotiations with the Council of the European Union.

[B] A Regulation, Not a 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. Due to the legal nature of a regulation under EU law, relying on a data protection regulation instead of a directive to establish a single rule that applies directly and uniformly, makes sense.

[1] Shortcomings of Directives

For a long time since the creation of the European Union, directives have been used to bring different national laws in line with each other. However, directives prescribe only an end result that must be achieved in every Member State. The form and methods of implementing the principles set forth in a directive are a matter for each Member State to decide for itself. 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. A directive only takes effect through national legislation that implements the measures.

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. When developing or revising their data protection laws to implement the data protection directives, the 27 Member States created a patchwork of 27 rules with different structures, different wording, and different basic rules. Some countries were very slow in implementing some of the directives. This fragmentation creates a significant burden on businesses, which are forced to act as a chameleon, and adapt to the different privacy rules of the countries in which they operate, or risk retaliation by the local or national data protection supervisory authorities.

[2] Benefits of Regulations

EU regulations are the most direct form of EU law. A regulation is directly binding upon the Member States and is directly applicable within the Member States. As soon as a

regulation is passed, it automatically becomes part of the national legal system of each Member State. There is no need for the creation of a new legislative text.

Because a regulation is directly applicable, as is, in the Member States, by adopting a Regulation for most data protection matters, the EU Commission intends to equip each of its Member States with the same basic legal instrument that applies uniformly to all companies, all organizations, and all individuals throughout the entire territory of the Union. The choice of a regulation for the new general regime for personal data protection is intended to provide greater legal certainty by introducing a harmonized set of core rules that will be the same in each Member State.

## § 6A.02 OVERVIEW OF THE PROPOSED REGULATION

The proposed provisions are laid out in a 119-page draft document. Among the most significant changes, the Proposed Regulation would change the rules for consent to require that there be an "explicit" consent. It would introduce some new concepts that were not in Directive 95/46/EC, such as the concept of breach of security, the protection of the personal information of children, the generalized use of binding corporate rules, the special status of health information, and the requirement that most corporations and government agencies hire a data protection officer. The Proposed Regulation would also require companies to conduct privacy impact assessments, to implement "Privacy by Design" rules, and to ensure "Privacy by Default" in their applications and products. Individuals would have greater rights, such as the "Right to be Forgotten" (or "Right to Erasure") and the "Right to Data Portability." Some of the key components of the Proposed Regulation are discussed below.

### [A] Provisions Affecting Businesses

The most significant provisions affecting businesses include:

- **Single Law Throughout 31 Countries:**
  The Regulation would establish a single law for data protection, replacing the current inconsistent patchwork of 31 national laws.
- **Extended Jurisdiction: Same Rules for all Companies,**

**Regardless of their Establishment:**

Under the Regulation, companies based outside of Europe will have to apply the same rules when operating in the European Union as the companies established in Europe.

- **One-Stop-Shop:**

  The Regulation would establish a "one-stop-shop" for businesses. Businesses would have to deal with one single data supervisory authority, not 31. It is expected that this simplification would make it simpler and cheaper for companies to do business in the EU.

- **Privacy by Design and Privacy by Default:**

  The Regulation would require the implementation of "Privacy by design" and "privacy by default" principles when designing or operating personal information databases. Data protection safeguards would have to be built into products and services from the earliest stage of development, and privacy-friendly default settings would have to be the norm.

- **Security Breach Notification:**

  Companies and organizations would be required to notify the national Data Protection Supervisory Authority of security breaches as soon as possible (24 to 72 hours currently proposed) so that users can take appropriate measures.

- **No more Notifications:**

  Businesses would no longer be required to notify their databases and personal data handling practices to Data Protection Supervisory Authorities.

- **Stronger Enforcement Powers for Data Protection Supervisory Authorities:**

  The fine levels available to data protection authorities will significantly increase. The initial text of the Proposed Regulation provides of fines 2% of their global annual turnover. The European Parliament has proposed 5%.

In addition, certain provisions are expected to apply only to large businesses, whereas small and medium sized enterprises (SME) would be exempt. These include:

- **Data Protection Officers:**
  Large businesses would be required to assign the responsibility for data protection to a specific "Data Protection Officer." SMEs would be exempt from this obligation if they process only a limited number of personal data.

- **Impact Assessments:**
  Business would be required to perform privacy impact assessments. However, SMEs would have no obligation to carry out an impact assessment unless there is a specific risk.

[B] Provisions Affecting Individuals

In addition to the rights already provided for in the 1995 Data Protection Directive, the Regulation would introduce new rights:

- **Right to Be Forgotten:**
  When an individual no longer wants his data to be processed and there are no legitimate grounds for retaining them, he would be able to ask for the deletion of the data.

- **Right of Portability:**
  A right to data portability would allow individuals to obtain the transfer of their personal data between service providers.

- **Express Consent Required**
  Consent to the processing of personal data will have to be express. Individuals must be asked to give it explicitly. It cannot be assumed.

## § 6A.03 SCOPE OF THE PROPOSED REGULATION

The material scope of the Proposed Regulation would generally be similar to that which currently exists—but for the fact that the Regulation would apply directly in each Member State. However, the territorial scope would be slightly extended. The Proposed Regulation makes it clear that its provisions would apply, as well, to certain foreign entities.

[A] Material Scope

Under Articles 1 and 2 of the Proposed Regulation, the new Regulation would govern the processing of personal data wholly or partly by automated means, and the processing other than by automated means of personal data that form part of a filing system or are intended to form part of a filing system. The processing of personal data by a natural person without any gainful interest and in the course of its own exclusively personal or household activity would be outside the scope of the Regulation, as this is the case currently under the 1995 Directive.

The Regulation would also not apply to the processing of personal data:

- In the course of activities that fall outside the scope of Union law, such as national security;
- By the Union institutions, bodies, offices and agencies;
- By the Member States when carrying out activities that fall within the scope of the rights reserved to the States;
- By competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offenses or the execution of criminal penalties.

Probably inspired by recent revelations over the extensive surveillance conducted by governmental security agencies throughout the world in their search for terrorist and other criminal activities, the proposed amendment in the LIBE Committee Report would increase the scope of the Proposed Regulation in several ways, in particular by removing the carve out of activities by national security agencies, and activities by EU institutions, bodies, offices, and agencies in the original text of the Regulation, and instead making these activities within the ambit of the General Data Protection Regulation.

On the other hand, the proposed amendment in the LIBE Committee Report would exclude from the scope of the Regulation the processing of personal data by natural persons in the course of exclusively personal or household activity but when this processing is in connection with the publication of personal data it can be reasonably expected that it will be only accessed by a limited number of persons. Among other things, this clarification

would help address whether, or the extent to which, information posted in social networks is subject to the Regulation.

[B] Territorial Scope

The provisions pertaining to the territorial scope of the proposed document make it clear that the Regulation is also intended to apply to entities that are not located on the EU territory, but whose activities pertain to, or directly affect, EU citizens.

[1] Processing by an EU Entity

The Regulation would apply to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, whether the processing takes place in the European Union or not.[5]

[2] Processing by a Foreign Entity

The Regulation would also apply to the processing of personal data by a data controller that is not established in the EU if (i) the data pertain to a data subject in the Union and (ii) the processing is performed by a controller that is not established in the Union, if the processing activities are related to:[6]

- The offering of goods or services to such data subjects in the Union; or
- The monitoring of their behavior.

The proposed amendment in the LIBE Committee Report would modify the above list to read as follows:

- The offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or
- The monitoring of such data subjects.

The Regulation would also apply to the processing of personal data by a controller that is not established in the Union, if the

[5]Proposed Regulation, Art. 3(1).
[6]Proposed Regulation, Art. 3(2).

processing occurs in a place where the national law of a Member State applies by virtue of public international law.[7]

## § 6A.04 PROTECTED INFORMATION

The Proposed Regulation would distinguish personal data in general, from data of a more sensitive nature, as this is the case under the 1995 Directive. Several additional categories of personal information would receive specific attention, such as personal data pertaining to children.

### [A] Personal Data

The data to be protected would be the same as those protected under the 1995 Directive. The term "personal data" is defined as "any information relating to a data subject."[8]

As generally understood under the 1995 Directive, a "data subject" would be an identified natural person or a natural person who can be identified, directly or indirectly, by means reasonably likely to be used by the controller or by any other natural or legal person, in particular by reference to an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.[9] The definition introduces the concept of "genetic data."

The proposed amendment in the LIBE Committee Report would slightly modify and enhance the definitions of the key terms used to identify the protected personal data.

Under the LIBE Committee Report, "data subject" would be defined as "a person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, unique identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social or gender identity of that person."[10] The definition excludes the protection of anonymous

---

[7]Proposed Regulation, Art. 3(3).
[8]Proposed Regulation, Art. 4(2).
[9]Proposed Regulation, Art. 4(1).
[10]Proposed Regulation, Art. 4(2).

data and introduces the concept of "genetic data."

The LIBE Committee Report would define the term "genetic data" as "all personal data relating to the genetic characteristics of an individual which have been inherited or acquired as they result from an analysis of a biological sample from the individual in question, in particular by chromosomal, desoxyribonucleic acid (DNA) or ribonucleic acid (RNA) analysis or analysis of any other element enabling equivalent information to be obtained."

The proposed amendment in the LIBE Committee Report would also provide new definitions for several concepts, which are absent from the draft General Regulation: pseudonymous data, encrypted data, and profiling. These definitions would be much welcome because the concepts are evolving with the adoption of new technologies and new uses of data, and it is often difficult to narrow down their application.

"Pseudonymous data" would be defined as "personal data that cannot be attributed to a specific data subject without the use of additional information, as long as such additional information is kept separately and subject to technical and organizational measures to ensure non-attribution."[11]

The concept of "encrypted data" would be defined as "personal data, which through technological protection measures is rendered unintelligible to any person who is not authorized to access it."[12] Unfortunately, this definition does not help because it fails to take into account that different forms of encryption generate different results.

Finally, the concept of "profiling" would be defined as "any form of automated processing of personal data intended to evaluate certain personal aspects relating to a natural person or to analyze or predict in particular that natural person's performance at work, economic situation, location, health, personal preferences, reliability or behavior."[13]

---

[11]Proposed Regulation, Art. 4(2a).
[12]Proposed Regulation, Art. 4(2b).
[13]Proposed Regulation, Art. 3(a).

[B] Special Categories of Data

While the basic definition of personal data would remain, the rules that apply to special categories of data or 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. Article 9 of the Proposed Regulation lists the following categories of data as requiring special protection: personal data, revealing race or ethnic origin, political opinions, religion or beliefs, trade-union membership, genetic data, data concerning health or sex life and data concerning criminal convictions or related security measures.

The proposed amendment in the LIBE Committee Report would expand further the above list of the "special categories" of data. With the changes to Article 9 proposed in the LIBE Committee Report, the following data would be part of the "special categories of data": data revealing race or ethnic origin, political opinions, religion or philosophical beliefs, sexual orientation or gender identity, trade-union membership and activities, genetic or biometric data, data concerning health or sex life, data concerning administrative sanctions, judgments, criminal or suspected offences, convictions or related security measures. This is a much broader range of data.

[1] Data of Children Under 13

The new Regulation would introduce the concept of the protection of children information. 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. The term "child" would be defined as an individual less than 13 years of age.

[2] Biometric Data

Biometric data would require special attention. If the processing would involve personal data in large-scale filing systems that include biometric data, a data protection impact assessment would be required to ensure that the processing is strictly limited to the activities permitted under the Regulation.[14]

[14]Proposed Regulation, Art. 33(2)(d).

The term "biometric data" is defined to include any data relating to the physical, physiological, or behavioral characteristics of an individual that allow their unique identification, such as facial images, or dactyloscopic data.[15]

[3] Sensitive Data

The definition of "sensitive data" would be expanded to include genetic data, and criminal convictions or related security measures.[16]

The notion of what constitutes "sensitive data" would continue to be significantly different from that which is used in the United States. In the United States, data that are generally identified as "sensitive" tend to be those that would result in identity theft in case of a loss or breach of security; e.g., credit card or driver's license information. In the European Union, the data that are deemed "sensitive" are those that might cause embarrassment or intrusion into a person's intimacy if the data were lost or exposed (e.g., information about health or sexual preference) or that may cause discrimination or retaliation (e.g., information about religion or trade union membership).

[4] 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. The special categories would include processing of personal data for:

- Journalistic purposes (Article 80);
- Health purposes (Article 81);
- Use in the employment context (Article 82);
- Historical, statistical or scientific purposes (Article 83);
- Access by a DPA to personal data and premises where data controllers are subject to an obligation of secrecy (Article 84); and

[15]Proposed Regulation, Art. 4(11).
[16]Proposed Regulation, Art. 9.

- Churches (Article 85).

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.

## § 6A.05 PROTECTED INDIVIDUALS

The protected individuals would be people in general or "data subjects," with special rules for the protection of children under 13. Individuals are protected to the extent that they are an "identified natural person" or a "natural person or a natural person who can be identified," directly or indirectly, by means reasonably likely to be used by the controller or by any other natural or legal person, in particular by reference to an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.[17]

## § 6A.06 COVERED ACTIVITIES

Like in the case under the 1995 Directive, the covered activities would be the different forms of processing. The term "processing" retains its existing, very broad definition. Under Article 4(3) of the Proposed Regulation, "processing" would be defined to include any operation or set of operations that is performed upon personal data or sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, erasure or destruction.

## § 6A.07 ENTITIES SUBJECT TO THE REGULATION

As under the 1995 Directive, the two categories of entities that are primarily the subject of the Regulation are the data "controller" and the data "processor." However, under the Proposed Regulation, the obligations and liabilities of the processors would be significantly increased. The Proposed Regulation would significantly reduce the distinction between controller and

[17]Proposed Regulation, Art. 4(1).

processor. The data processors would be subject to almost the same obligations as the data controllers and would be exposed to the same liability, damages, and sanctions.

## § 6A.08 GENERAL RULES GOVERNING PERSONAL DATA PROCESSING

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. 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.

### [A] Basic Principles

The seven basic principles relating to data processing would require that the personal data be:[18]

- 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; and
- Processed under the responsibility and liability of the data controller, who must ensure and demonstrate for each operation its compliance with the Regulation.

The LIBE Committee Report provides a slightly different definition of the basic principles. Under the proposed amendment in the LIBE Committee Report, there are nine rather than seven

[18]Proposed Regulation, Art. 5.

principles and their modified wording provides that personal data should be processed as follows:

- Processed lawfully, fairly, and in a transparent manner in relation to the data subject (lawfulness, fairness, and transparency);
- Collected for specified, explicit, and legitimate purposes, and not further processed in ways incompatible with these purposes (purpose limitation);
- Adequate, relevant, and limited to the minimum necessary (data minimization);
- 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 and, where necessary, kept up to date, with incorrect data being erased or rectified (accuracy);
- Kept in a form that permits direct or indirect identification of the data subjects for no longer than necessary; personal data may be stored for longer periods insofar as the data will be processed solely for historical, statistical, or scientific research or for archive purposes in accordance with the rules and conditions of Articles 83 and 83(a) and if a periodic review is carried out to assess the necessity to continue the storage, and if appropriate technical and organizational measures are put in place to limit access to the data only for these purposes (storage minimization);
- Processed in a way that effectively allows the data subject to exercise his or her rights (effectiveness);
- Processed in a way that protects against unauthorized or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organizational measures (integrity);
- Processed under the responsibility and liability of the data controller, who shall ensure and be able to demonstrate its compliance with the Regulation (accountability).

[B] Specific, Informed, and Explicit Consent

One of the significant differences with Directive 95/46/EC is that the notion of consent would be strengthened. Currently, in most EU Member States, consent is implied in many circumstances. For example, in most countries, an individual who uses a website is often assumed to have agreed to the privacy policy of that website.

Under the new regime, when processing is based on consent, the consent will have to be "specific, informed, and explicit" (Article 7). The controller would have to bear the burden of proving that the data subjects have given their consent to the processing of their personal data for specified purposes. 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 again for this consent.

This evolution is consistent with the way the European laws have changed in past few years, with the new stringent requirements for cookies under the 2009 amendments to Directive 2002/58/EC.[19] The amendment to Section 5(3) of the 2002 privacy Directive has caused the EU Member States to modify their national laws to require that the user's specific (opt-in) consent be obtained before cookies, other than technical cookies, can be sent to the user's computer. Before the 2009 amendments, cookies were subject to less stringent restrictions, and could be used without a formal consent of the user. It was only necessary to inform them of their right to refuse the use of cookies and their ability to block access to their computers.

## § 6A.09 OBLIGATIONS OF CONTROLLERS AND PROCESSORS

Articles 22 through 29 would 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.

---

[19] *See* Chapter 7, "2002 EU Directive on Privacy and Electronic Communications."

[A] Responsibility and Accountability

Article 22 addresses the responsibility of the controllers. Under the Proposed Regulation, the data controller would be deemed "responsible" for the data. It would have 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. These measures would include, for example, the following obligations for the data controller:[20]

- The obligation to keep documents;
- The obligation to implement data security measures;
- The obligation to perform a data protection impact assessment in special circumstances;
- The obligation to implement mechanisms to ensure the verification of the effectiveness of the measures described above. This may require retaining an independent auditor to conduct the verification; and
- The obligations of the data controller to ensure data protection by design and by default.

The LIBE Committee Report adds to the notion of "responsibility" that of "accountability." This concept slightly resembles the concept of accountability found in the APEC Privacy Framework.[21] The term "accountability" has been added throughout the text of the proposed amendments set forth in the LIBE Committee Report. In the LIBE Committee Report approach, "accountability" is presented as a process that incentivizes good organizational practices. For example, the proposed new Recital 61(a) provides:

> (61a) This Regulation encourages enterprises to develop internal programmes that will identify the processing operations likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature,

[20]Proposed Regulation, Art. 22(2).

[21]*See* Chapter 10, "The Asia-Pacific Region."

> their scope or their purposes, and to put in place appropriate privacy safeguards and develop innovative privacy-by-design solutions and privacy enhancing techniques. Enterprises that can publicly demonstrate that they have embedded privacy accountability do not also require the application of the additional oversight mechanisms of prior consultation and prior authorisation.

As a result, the proposed amendment in the LIBE Committee Report would drastically change the general and vague statements of Article 22(1) and replace the provision by a more comprehensive and specific mandate in subsection (1) and a new subsection (1a):

> 1. The controller shall adopt appropriate policies and implement appropriate and demonstrable technical and organisational measures to ensure and be able to demonstrate in a transparent manner that the processing of personal data is performed in compliance with this Regulation, having regard to the state of the art, the nature of personal data processing, the context, scope and purposes of the processing, the risks for the rights and freedoms of the data subjects and the type of the organization, both at the time of the determination of the means for processing and at the time of the processing itself.
>
> 1a. Having regard to the state of the art and the cost of implementation, the controller shall take all reasonable steps to implement compliance policies and procedures that persistently respect the autonomous choices of data subjects. These compliance policies shall be reviewed at least every two years and

updated where necessary

The amendment proposed in the LIBE Committee Report would remove the costly audits and verification and audits provided in the original Article 22(3) and replace it with a requirement that all data controllers be able to demonstrate the adequacy and effectiveness of the measures listed above.

Further, the proposed amendment to Article 22(3), in the LIBE Committee Report, would require that any regular general reports of the activities of the controller, such as the obligatory reports by publicly traded companies, contain a summary description of the policies and measures listed above.

Because of this emphasis on accountability, the proposed amendment in the LIBE Committee Report would also remove, among other things, the powers that are granted to the Commission, in the original Article 22(4), to adopt delegated acts in order to specify additional criteria, auditing, or verification to supervise the activities of the data controllers and processors.

[B] Data Protection by Design and by Default

"Data protection by design" and "data protection by default" are among the new concepts introduced in the Proposed Regulation.

[1] Data Protection by Design

Article 23 of the Proposed Regulation would require the data controller, both at the time of the determination of the means for processing and at the time of the processing itself, to implement appropriate technical and organizational measures and procedures to ensure that the processing will meet the requirements of the Regulation and ensure the protection of the rights of the data subject. Since the Proposed Regulation tries to be technology neutral and general, it specifies that this requirement must take into account the state of the art and the cost of implementation but does not specify particular methods or steps to be taken.

The proposed amendment in the LIBE Committee Report would set forth a much more comprehensive Article 23. First, the criteria for the proper methodologies for the process of "data

protection by design" would be significantly expanded and refined. These would include, in addition to the state of the art, already mentioned in the original draft, the current technical knowledge, international best practices, and the risks represented by the data processing.

Further, the proposed amendment in the LIBE Committee Report would require that both the controller and the processor, if any, implement appropriate and proportionate technical and organizational measures and procedures both at the time of the determination of the purposes and means for processing and at the time of the processing itself.

The LIBE Committee Report would also require that data protection by design processes and methodologies have particular regard to the entire lifecycle management of personal data from collection to processing to deletion. In addition, it would require that data holders systematically focus on comprehensive procedural safeguards regarding the accuracy, confidentiality, integrity, physical security, and deletion of personal data. Further, the proposed LIBE Report amendment would also require that the result of any data protection impact assessment[22] be taken into account when developing those measures and procedures.

[2] Data Protection by Default

Article 23(2) would require data controllers to implement mechanisms for ensuring that, by default, the processing be limited to only those personal data that are necessary for each specific purpose of the processing. Data controllers would also be required to ensure that data are not collected or retained beyond the minimum necessary for the specific purposes for which they were collected, both in terms of the amount of the data and the duration of their storage or retention.

Article 23 stresses in particular that the data controller must ensure that by default personal data are not made accessible to an indefinite number of individuals. This provision would affect, for example, social networks, which tend to set default setting to choices that would make individuals' personal data available to

[22]Privacy Impact Assessments are addressed in Article 33 of the Proposed Regulation.

large circles of individuals, if not, the public at large.

The proposed amendment in the LIBE Committee Report would increase the protection provided in Article 23 and require that data controllers ensure that data are not disseminated beyond the minimum necessary for the specific purposes for which they were collected. It would also require that the data controller ensure that, by default, the data subjects are able to control the distribution of their personal data.

[C] Data Protection Impact Assessment

While the Proposed Regulation would relax some of the administrative burden, such as the notification requirements, 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.

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.

[D] Joint Controllers

Articles 24 and 25 would 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. Under Article 24, joint data controllers would be required to determine their own allocation of responsibility for compliance with the Regulation. If they fail to do so, they would be held jointly responsible. Article 25 would require data controllers that are not established in the European Union, when their data processing activities are subject to the Regulation, to appoint a designated representative in the European Union.

[E] Data Processors

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 the case, data processors would be directly prohibited from processing personal data other than pursuant to the data controller's instructions.

Article 26 would build on Article 17(2) of Directive 95/46/EC and increase the obligations of the data processors. 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. This very important clarification is consistent with Working Paper WP 169 issued by the Article 29 Working Party in March 2010. In this paper, the Article 29 Working Party discussed when a data processor becomes a joint controller with the initial data controller.

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 on the client agreeing to a contractual provision in which the client acknowledges that the cloud service provider is a data processor and not a data controller. If a cloud service provider chooses 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?

## § 6A.10 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. 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."

[A] 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 data controllers 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.

The proposed amendments in the LIBE Committee Report would result in a series of changes and clarifications to Articles 11 and 12 of the original draft Regulation. For example, the notice obligation set forth in Article 11 of the Proposed Regulation would be expanded to require that the data controllers' notice to the data subjects be concise and clear in addition to being transparent. The proposed changes to Article 12 would require that, where personal data are processed by automated means, data controllers provide data subjects with means for requests to be made electronically where possible. Currently many companies only offer access to data through written request, sent by mail, which acts as a deterrent, and creates a significant barrier to access the data.

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 months for responding.

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. 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. 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. 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.

[B] Right of Information

The right of information would be expanded from the current Articles 10 and 11 of Directive 95/46/EC, to entitle the data subject to receive more information than is currently required under the 1995 Directive. For example, individuals would have to be informed of the length of the period during which the data controller intends to hold their data. 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.[23]

[C] 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.[24]

[D] Right of Rectification

Article 16 would continue the right of rectification, which is defined in Article 12(b) of Directive 95/46/EC.

[E] Right to Object to the Processing

Article 14 of Directive 95/46/EC contains a right to object to the processing of personal data. This right would be provided by Article 19 of the Proposed Regulation. Changes from the 1995 version would pertain to burden of proof and direct marketing. It is not clear 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 and contains

[23]Proposed Regulation, Art. 14.
[24]Proposed Regulation, Art. 15.

a dual opt-in/opt-out process.[25]

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

The amendment proposed in the LIBE Committee Report would significantly modify Article 20. First, it would change the nature of the right. The original text provides for a right for "every natural person" not to be subject to a measure that "produces legal effects concerning [the] natural person or significantly affects" the natural person. The LIBE Committee Report proposed definition would refer to a "data subject" instead of a "natural person," and would provide for a right not to be subject to a measure that "adversely affects this data subject, both offline and online."

The LIBE Committee Report also suggests to expand Article 20. A new Article 20(1a) would provide that user profiles may be created for the purposes of advertising, market research, or tailoring telemedia, by using pseudonymised data, if the concerned individual does not object. Of course, the individual must be informed of his/her right to object. To preserve anonymity, user profiles would not be able to be combined with data about the bearer of the pseudonym.

According to the LIBE Committee comments, this addition is intended to address the fact that the original version might have required companies to obtain consent for any form of processing personal data. The LIBE Committee Report indicates that it believes that certain forms of data processing should be allowed with due respect to the protection of personal data in order not to destroy the business models of small and medium-sized European companies.

---

[25] *See* Chapter 7, "2002 EU Directive on Privacy and Electronic Communications."

[G] 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. 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. 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.

The LIBE Committee Report proposed amendment would change the name "right to be forgotten" and return to the initial concept of "right to erasure." It would grant data subjects the right to obtain from third parties the erasure of any links to, or copy or replication of their data, in addition to the currently planned 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. The proposed amendment would also remove the requirement that the data controller who has shared or disclosed the personal data inform third parties of the data subject's request to erase any links to, or copy of the data. Lobbyists from numerous companies had indicated that this latter requirement would be very difficult and very costly to implement.

[H] Right to Data Portability

Article 18 would introduce the data subject's right to "data portability," i.e., the right to transfer data from one automated processing system to, and into, another, without being prevented from doing so by the data controller. This right would include the right to obtain one's data from the controller in a structured and commonly used electronic format. The Proposed 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 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. Users of social networks have found out, to their detriment, that the ease of use of a social network and the access to the service for no fee was tied to a price: that their personal data could be used in forms or formats 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.

From a company's perspective, it is not clear how and to what extent the right to be forgotten and the right to data 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 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 backup 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, for example, if the company keeps a log of its data transfers.

The proposed amendment in the LIBE Committee Report would delete Article 18 discussed above in its entirety, and instead, append to Article 15 a new Article 15(2), which would provide for a right to transfer data from one automated processing system to, and into, another, without being prevented from doing so by the data controller. Article 15 would be renamed to provide for both the right to access personal data, and the right to obtain personal data.

Under this new Article 15(2) the data subject would have the right to obtain from the controller a copy of the provided personal data in an electronic and interoperable format that is commonly used and allows for further use by the data subject. Where technically feasible and available, the data would have to be transferred directly from controller to controller at the request of the data subject. The LIBE Committee Report 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 platform.

## § 6A.11 SECURITY AND CONFIDENTIALITY

Articles 30 through 32 would focus on the security of the personal data. They would include two major changes to the current regime. One is that data processors would be required by law to implement appropriate security measures, while in the current regime under the 1995 Directive, their obligations come mostly from contractual obligations. The other major change is the introduction of a general requirement to disclose security breaches.

### [A] 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. This provision is likely to affect, among others, certain cloud computing agreements where the cloud service provider places on the client the sole burden of providing adequate security, and disclaims any liability for loss of the data.

### [B] Security Breach Disclosure

In addition, the Proposed Regulation introduces an obligation to provide notification of "personal data breaches." 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."[26]

#### [1] Notification of the Data Protection Supervisory Authority

In case of a breach of security, a data controller would be required to inform the supervisory authority within 24 hours, if feasible.[27] A data processor that is the victim of a breach would

[26]Proposed Regulation, Art. 4(9).

[27]Proposed Regulation, Art. 31.

also be required to alert and inform the data controller immediately after establishing that a breach of security occurred.[28]

The proposed amendment in the LIBE Committee Report would provide for an approach that is much more business friendly. In case of a breach of security, a data controller would be required to notify the Supervisory Authority "without undue delay" instead of within 24 hours after discovery of the incident. Similarly, a data processor would be required to notify the concerned data controller also "without undue delay" instead of "immediately."

[2] Notification of the Data Subjects

In addition, if the breach were "likely to adversely affect the protection of the personal data or the privacy of the data subject," the data controller would be required to notify the data subjects, without undue delay, after it has notified the supervisory authority of the breach.[29] 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.[30]

## § 6A.12 TRANSFER OF PERSONAL INFORMATION OUT OF THE COUNTRY

For most global companies, a critical aspect of the EU data protection laws is whether and in which manner the national law of a country permits or 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 EEA and to most of the rest of the world is prohibited unless an exception applies. This rule would remain. However, the Proposed Regulation would provide for simplification. Some of the key aspects of the plan include putting in place a "one-stop-shop" approach, removing the discrepancies in the regimes for cross-border data transfers, and validating the use of binding corporate rules in all Member States.

---

[28]Proposed Regulation, Art. 31(2).

[29]Proposed Regulation, Art. 32.

[30]Proposed Regulation, Preamble, Recital 67.

[A] General Principles for Transfers

The general rules for the transfer of personal data out of the European Union would be generally consistent with—albeit, slightly less cumbersome than—those that are stated in Articles 25 and 26 of the 1995 Directive.[31] Simply put, the transfer of personal data out of the EU or EEA is prohibited unless the recipient country provides "adequate protection" to personal data and the privacy rights of individuals. Only a handful of countries have been deemed by the European Commission to provide "adequate protection." For transfers of data to the other countries, the recipient must enter into a written contract in which the recipient of the data commits to doing, or to refrain from doing, certain acts. The European Commission has approved certain forms of contracts. In addition, a majority of the EU Member States—but not all of them—currently recognize "binding corporate rules" as a way for a group of companies to express their commitment to provide and ensure the required "adequate protection" even when the recipient is located in a country that does not offer this "adequate protection."

In the Proposed Regulation, the conditions of, and restrictions to, data transfers to third countries or international organizations, including onward transfers, would be defined in Articles 40 through 45. For transfers to third countries that have not been deemed to provide "adequate protection," Article 42 would require that the data controller ***or data 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 also be adopted by a supervisory authority and be declared generally valid by the Commission;
- Binding corporate rules are specifically introduced as a legitimate ground for allowing for the transfer of personal information out of the European Economic Area. Currently they are only accepted in about 17 Member States while in other Member States they are illegal;

[31] *See* Chapter 9, "Transferring Personal Data out of the European Union and European Economic Area."

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

Article 44 would spell out and clarify the derogations for a data transfer. These conditions are based on Article 26 of Directive 95/46/EC. 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.

Article 45 would provide 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 (Draft 56 of the Proposed Regulation, dated November 29, 2011), has been removed. This article provided that foreign judgments requiring a controller or processor to disclose personal data would not 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. It required a controller or processor to immediately notify the supervisory authority of the request and to obtain prior authorization for the transfer. It is not clear why the provision was removed and whether this issue will be addressed separately.

[B] Binding Corporate Rules

Binding corporate rules would take a prominent place in the Proposed Regulation. Their required content is outlined in Article 43. An organization's binding corporate rules would have to contain the following information:

- The structure and contact details of the entities in the group;
- The categories of personal data, the type of processing and its purposes;
- The type of data subjects affected;
- The third countries where data are to be sent;
- Their legally binding nature, both internally and externally;

- The general data protection principles, in particular purpose limitation, data quality, legal basis for the processing, processing of sensitive personal data; measures to ensure data security; and the requirements for onward transfers to other organizations;
- The rights of data subjects and the means to exercise these rights, including the right to obtain redress and compensation for a breach of the binding corporate rules;
- The acceptance by the controller or processor established on the territory of a Member State of liability for any breaches of the binding corporate rules by any member of the group not established in the Union;
- How the information on the binding corporate rules is provided to the data subjects;
- The tasks of the data protection officer;
- The mechanisms to be used in order to ensure compliance with the binding corporate rules;
- The mechanisms for reporting and recording changes to the policies and reporting these changes to the supervisory authority; and
- The cooperation mechanism with the supervisory authority.

## § 6A.13 DOCUMENTATION REQUIREMENTS; SUPERVISION BY DATA PROTECTION AUTHORITY

The Proposed Regulation would significantly reduce the administrative burden, and the related expenses, that result from the obligation to report to each local data protection authority the existence of a database of personal information, and the proposed processing activities.

### [A] No More Notification Requirement

The Proposed Regulation would eliminate the requirement to notify the Data Protection Authority. This requirement was viewed as cumbersome, in particular for entities with operations in several states. Under the national data protection laws that implement the 1995 Directive, companies have to file notifications in each of the

countries where they operate. The requirements for these notifications, the forms to be used, and the information to be disclosed, the cost and periodicity of the filing, and the exceptions to the conditions for filing notifications differ from country to country.

Instead of the notification requirement, the Proposed Regulation would require both data controllers and data processors to keep substantial records, written policies, and other information, and to promptly respond to inquiries by the data protection supervisory authorities.

[B] Documentation Requirement

Article 28 would detail 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.

The proposed amendment in the LIBE Committee Report would require that the documentation be "regularly updated."

This removal of the notification requirement reflects a significant shift in the attitude of the European Commission, which is expressed throughout the Proposed Regulation: a switch from tight supervision and reporting to a concept of accountability. In exchange for abolishing the cumbersome and costly notification requirement, the new Regulation would require that data controllers and data processors be "accountable." They would be trusted to create their own structures, but they would have to document them thoroughly. They would also have to be prepared to respond to any inquiry from the Data Protection Authority, to promptly produce the set of rules with which they have committed to comply, and to show that they do actually comply with the provisions of the Regulation.

Article 28 identifies a long list of documents that would have to be created and maintained by data controllers and data processors. The information required is somewhat similar to the information that is currently provided in the notifications to the

data protection authorities—e.g., the categories of data and data subjects affected, or the categories of recipients. There are, however, also 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.

[C] Cooperation with Supervisory Authority

Article 29 would require data controllers, data processors, and, as applicable, the data controller's local representative, to cooperate, on request, with the supervisory authority in the performance of its duties. In particular, they will have to provide access to all personal data and all information required by the supervisory authority, as well as to their premises and data processing equipment in response to access requests made by the supervisory authorities in the exercise of their investigative powers.

[D] Main Establishment

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 processor or data controller has its "main establishment" would be competent for supervising the processing activities of that processor or controller in all Member States where the company or group of companies operate, subject to the mutual assistance and cooperation provisions that are set forth in the Proposed Regulation.

The proposed amendment in the LIBE Committee Report would modify the definition of "main establishment," in Article 4(13). Under the revised definition, a "main establishment" would be "the place of establishment of the undertaking or group of undertakings in the Union, whether controller or processor, where the main decisions as to the purposes, conditions and means of the processing of personal data are taken." Further, the definition would apply both to data controllers and to data processors.

In addition, the proposed amendment in the LIBE Committee Report would provide objective criteria that may be used to determine the main establishment of the controller or processor.

These criteria would include:

- The location of the controller or processor's headquarters;
- The location of the entity within a group of undertakings that is best placed in terms of management functions and administrative responsibilities to deal with and enforce the rules as set out in the Regulation; and
- The location where effective and real management activities are exercised determining the data processing through stable arrangements.

[E] 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. The controller or processor acting on the controller's behalf would have to consult the supervisory authority before the processing of personal data in order to ensure that the intended processing complies with the Regulation. This would be the case, in particular, where a data protection impact assessment indicates that processing operations might present a high degree of specific risks, or if the supervisory authority deems it necessary to carry out a prior consultation on processing operations that are likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, scope or purpose.

In addition, the data controller or the processor would be required to obtain an authorization from the supervisory authority prior to the processing of personal data in the case of certain cross-border transfers of personal data if it uses contractual clauses other than the standard pre-approved clauses or does not provide for the appropriate safeguards in a legally binding instrument for the transfer of personal data to a third country or an international organization.

## § 6A.14 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. 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, already require organizations to hire a Data Protection Officer, who is responsible for the company's compliance with the national data protection law. In the United States, numerous laws and FTC consent decrees require entities to appoint a Data Protection Officer to be responsible for all matters pertaining to data protection within the entity.

## § 6A.15 COMPLAINTS, JUDICIAL REMEDIES

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.

### [A] 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.

### [B] Judicial Remedy Against Data Controllers or Processors

In addition to the administrative remedies, e.g., complaint with a supervisory authority, individuals would have a private right of action against a data controller or a data processor. Article 75 would allow them 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.

The proposed amendment in the LIBE Committee Report

would carve out from the ability to bring a case to court the cases where the data controller is a public authority of the Union or a Member State acting in the exercise of its public powers.

[C] 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 (DPA) to act on a complaint. The courts of the Member State where the DPA is located would be competent to hear the matter. In addition, it would allow the DPA 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) DPA is established in order to require that it take action.

[D] Class Actions-Like Initiatives

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.[32]

The wording proposed in the LIBE Committee Report would modify the definition of the organizations allowed to initiate these actions. The original draft Regulation grants this right of action to "any body, organization or association that aims to protect data subjects' rights and interests concerning the protection of their personal data and has been properly constituted according to the law of a Member State." The proposed amendment in the LIBE Committee Report would grant this right to "any body, organization, or association that acts in the public interest and has been properly constituted according to the law of a Member State."

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. These group actions could be initiated against data controllers or data processors that have infringed their members'

[32]Proposed Regulation, Art. 73.

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 are familiar. Many of the class actions currently filed in the United States cause great expenses to companies, and frequently bring little relief to the actual injured parties or the named plaintiffs. 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 attorney 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.

## § 6A.16 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 individuals with a right to compensation, and set significant penalties and administrative sanctions against data controllers and data processors.

### [A] 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***, as applicable, for the damages suffered. Instead of "damages," the proposed amendment in the LIBE Committee Report would grant the right to "claim compensation," which could be "pecuniary or not."

When more than one entity is involved in the processing, the controllers and processors involved in the processing would be held jointly and severally liable for the entire amount of the damages. The proposed amendment in the LIBE Committee Report would carve out from this joint and several liability the instances where the parties have an appropriate written agreement determining their responsibilities.

[B] Significant Penalties

Articles 78 and 79 would address penalties and sanctions. According to the Regulations, these penalties would have to be "effective, proportionate and dissuasive." 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. The provision targets in particular the failure by a foreign entity to appoint a local representative. Where a representative has been established, the penalties would be applied first to the representative.

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 sanction 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.

The proposed amendment in the LIBE Committee Report provides a much wider range of criteria to be used to determine sanctions. These criteria would include the following:[33]

- Nature, gravity, and duration of the incompliance;
- Intentional or negligent character of the infringement;
- Degree of responsibility of the natural or legal person and of previous breaches by this person;
- Repetitive nature of the infringement;
- Degree of cooperation with the supervisory authority in order

[33]LIBE Committee Report, Art. 79(2c).

to remedy the infringement and mitigate the possible adverse effects of the infringement;

- Specific categories of personal data affected by the infringement;
- Level of damage, including non-pecuniary damage suffered by the data subjects;
- Actions taken by the controller or processor to mitigate the damage suffered by data subjects;
- Financial benefits intended or gained, or losses avoided, directly or indirectly from the infringement;
- Degree of technical and organizational measures and procedures implemented in application of other provisions of the Regulation, such as data protection by design and by default, security measures, data protection impact assessment, data protection compliance review, designation of a data protection officer;
- Refusal to cooperate with or obstruction of inspections, audits, and controls carried out by the supervisory authority;
- Other aggravating or mitigating factors applicable to the circumstance of the case.

The Proposed Regulation would specify significant sanctions for 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. This is much more than the penalties currently in place throughout the European Union. Apart from a few cases, the level of fines that have been assessed against companies that violated a country's data protection laws has been low, even though it has periodically increased. The Proposed Regulation signals an intent to pursue more aggressively 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 up to .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.

- **Fines up to 500,000 Euros or up to 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.
- **Fines up to 1,000,000 Euros or up to 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.

The proposed amendment in the LIBE Committee Report would provide much more significant sanctions and penalties than the draft proposed by Viviane Reding. Under the LIBE Committee Report proposal, the Supervisory Authority would have the right to impose at least one of the following sanctions:

- **A warning in writing** in cases of first and non-intentional non-compliance;
- **Regular periodic data protection audits**;
- **A fine up to 100,000,000 EUR or up to 5% of the annual worldwide turnover** of an enterprise, whichever is greater.

## § 6A.17 DATA PROTECTION SUPERVISORY AUTHORITY

The Proposed 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 as independent entities, and would receive additional powers. Their mission would be enlarged and they would be required to cooperate with each other. The Article 29 Party would have increased authority and a new name, better suited to its role.

### [A] 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 DPA's mission and require them to cooperate with each other and with the European Commission and to implement the relevant case law.[34]

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 DPAs, and the regulations governing the duties of the members and staff of the DPA.

Article 51 would set out the competence of the DPAs while Article 52 and 54 would define their duties and Article 53 their powers. The competence of each DPA would be limited to its own national territory in most cases. However, in the case of data processors or data controllers established in several countries, the DPA of the principal establishment of the corporate group would acquire a new competence as the lead authority for that corporate group.

As this is currently the case, the duties of the DPAs would include hearing and investigation of complaints, raising public awareness of the rules, safeguards and rights, and preparing annual reports.[35] The proposed powers of the DPA 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.

[B] Cooperation and Consistency

The Proposed Regulation sets forth a series of rules that may help ensure cooperation and consistency among the DPAs. 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

[34]Proposed Regulation, Art. 20, 47, and 48.
[35]Proposed Regulation, Art. 52 and 54.

Member States. In some cases, unity and consistency may be obtained through opinions of the European Data Protection Board, discussed below.[36] There are also provisions giving the European Commission the power to intervene.[37]

## § 6A.18 EUROPEAN DATA PROTECTION BOARD

The "European Data Protection Board" would be the new name for the "Article 29 Working Party." The new Board would consist of the European Data Protection Supervisor and the heads of the supervisory authority of each Member State.[38] 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. However, the European Commission would have the right to participate in the activities and to be represented.

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 includes the obligation to adopt rules of procedure. Article 71 sets out a Secretariat of the European Data Protection Board. The service would be provided by the European Data Protection Supervisor.

## § 6A.19 POSSIBLE DIVERGENCE AMONG THE MEMBER STATES?

### [A] Is Uniformity Possible?

While on paper relying on a Regulation in order to force or instill more uniformity amongst the EU Member States may seem a great scheme, it remains to be seen how these fiercely independent countries, judges, lawyers or government officials will implement the new single rule, if any. Further, there are numerous circumstances—described below—where the Proposed Regulation would grant Member States the ability to enact their own rules or laws. This additional freedom is likely to be used, especially in those countries that have already expressed

[36]Proposed Regulation, Art. 58.
[37]Proposed Regulation, Art. 59 to 63.
[38]Proposed Regulation, Art. 64.

reservations on the content and substance of the Proposed Regulation.

The United States may be an example of this constant quagmire. The United States has numerous federal laws that are intended to apply uniformly in all of its states and territories. However, interpretations may vary significantly from one geographic area to another due to the cultural, economic and other numerous circumstances. Even though for more than 220 years, the U.S. Supreme Court has been trying to remove these discrepancies and even out the field, the same laws continue to be interpreted differently throughout the U.S. states and territories as evidenced by the frequent attempts at forum shopping by shrewd plaintiffs. It would not be surprising if the data protection commissioners, the government agencies, and the judicial system in each EU Member State also have differing interpretations of the same text.

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 or less numerous than those that are currently found among the Member State data protection laws. Nevertheless, once the final text becomes effective, it will be imprudent and very risky to act as if there were total uniformity.

[B] Ability to Create Additional Restrictions

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

Article 21(1) allows Union or Member State law to restrict by way of a legislative measure the scope of the obligations and rights provided for in Article 5(a) to (e), Articles 11 to 20 and Article 32, when such a restriction constitutes a necessary and proportionate measure in a democratic society to safeguard:

- Public security;
- The prevention, investigation, detection and prosecution of criminal offenses;

- Important economic or financial interests of the Members State or of the European Union, such as monetary, budgetary and taxation matters, and the protection of market stability and integrity;
- The prevention, investigation, detection or 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.

The view taken in the LIBE Committee Report is slightly more specific and narrower. In its version of Article 21(1), the LIBE Committee Report would provide that Union or Member State law may restrict by way of a legislative measure the scope of the obligations and rights in Articles 11 to 19 and Article 32, when such a restriction meets a "clearly defined objective of public interest, respects the essence of the right to protection of personal data, is proportionate to the legitimate aim pursued and respects the fundamental rights and interests of the data subject and is necessary and proportionate measure in a democratic society to safeguard" the concepts listed above (with slight modifications).

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 and the repeal of their national laws that implement the 1995 Directive. 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, 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 life, and a new interest from Member States who may take advantage of the provision to regain some of 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. The UK Data Protection Commissioner has also complained that the Draft Regulation needed to be strengthened and that it would create compliance and enforcement problems.

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, of course, difficult to predict at this point.

[C] 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 a tension between the right of privacy and the freedom of expression. This issue would subsist, and states would have the freedom to limit privacy rights to address freedom of information. 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.[39] The scope of the power

[39]Proposed Regulation, Art. 80.

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.

[D] 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,[40] the protection of employee personal data in the employment context,[41] rules regarding interaction with professionals having an obligation of secrecy[42] and the collection of personal data by churches and religious associations.[43]

[E] Operation of the Data Protection Supervisory Authorities

Divergences should be expected, as well, in the rules that pertain to the operations of the supervisory authorities. Articles 46 to 49 would grant the Member States the power to appoint one or several data protection authorities to be responsible for the monitoring of the application of the Regulation. The Member States would have the power to define the rules of operation of the data protection supervisory authorities 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.

[F] 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.

---

[40]Proposed Regulation, Art. 81.
[41]Proposed Regulation, Art. 82.
[42]Proposed Regulation, Art. 84.
[43]Proposed Regulation, Art. 85.

## § 6A.20 DELEGATED ACTS

Most of the provisions of the Proposed Regulation are intended to create a new uniform, data protection regime that takes into account the dramatic evolution of the way in which personal data is used, collected, stored, shared, or processed and that will remain in force for the next 15 to 20 years. However, the document, once fully adopted and implemented would not be set in stone. Numerous provisions of the Draft Regulation grant the European Commission the power to make changes and issue new provisions through "delegated acts" which might receive limited review. This is achieved through a "delegation of power" that allows the Commission the authority to issue "delegated acts" allegedly to modify, adapt, or clarify the regulation.[44] The original draft of the Proposed Regulation provides for 26 different areas in which the EU Commission can supplement and modify the Regulation "for an indeterminate period of time."

If all the proposed amendments in the LIBE Committee Report were implemented as is, the number of these permitted delegated acts would be reduced to 7 instead of 26.

## § 6A.21 NEXT STEPS

The terms of the Proposed Regulation are not a major surprise. In numerous documents, Viviane Reding, Vice-President of the European Commission and others have provided numerous descriptions of their vision for the new personal data protection regime. It is nevertheless exciting to see the materialization of these descriptions, outlines, and wish lists.

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 would help simplify the information governance, procedures, record keeping, and other requirements for companies 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.

[44]Proposed Regulation, Art. 86.

However it is likely that this dream might not become reality in the near future because the European Union Member States are fiercely independent, have their own culture, and their own past, and it is expected that they will keep interpreting the new provisions in their own way, or will seize every available opportunity to create an exception. The current draft of the Regulation contains numerous provisions that give each member state the ability to create its own set of rules.

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. It remains to be seen what effect the adoption of the Regulation will have on the data protection laws of these other countries.

With the overwhelming support of the EU Parliament, on March 12, 2014, the draft Data Protection Regulation has received an important vote of confidence. There will be now more pressure on the Council of the European Union to clear differences and move along, and finalize a draft. It is still difficult to predict when the Regulation will be finalized, and in what form or format.

## § 6A.22 THE RIGHT TO BE FORGOTTEN TAKES OFF

While the proposed Regulation is still being discussed, and the content of the final draft is still uncertain, a concept of "Right to be Forgotten," similar to that which is outlined in the Proposed Regulation and the LIBE Committee Report has already taken a life of its own as a result of a case against Google Spain and Google, Inc. which was brought to the Court of Justice of the European Union.[45]

The case started as a complaint against a Spanish newspaper, Google Spain, and Google Inc. by an individual who was concerned that a Google search for information about him would

[45]http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf.

display links to an announcement concerning an auction for the recovery of debts that he owed. The event had occurred, and the matter had been fully resolved more than ten years ago, and he argued that the display of this information was an infringement of his privacy rights. The case was subsequently submitted to the Court of Justice of the European Union, which found that in certain circumstances, an individual has a "right to be forgotten." This case and the ruling, as well as the subsequent activities of the Data Protection Authorities are very important because they are helping frame—in advance of the adoption of the Proposed Regulation—the rules that are likely to apply when implementing the Right to be Forgotten provisions of the General Data Processing Regulation.

[A] Court of Justice of the European Union: Google Spain SL, Google Inc. v. Agencies Española de Protección de Datos

In 2010, Mario Costeja Gonz´alez, a Spanish citizen filed a complaint against La Vanguardia Ediciones SL (a Spanish newspaper), Google Spain and Google Inc. with the Spanish Data Protection Authority. The individual complained that when an Internet user entered his name in the Google search engine, the list of results would display links to two pages of La Vanguardia's newspaper of January and March 1998. These pages contained an announcement concerning a real estate auction of his repossessed home for the recovery of social security debts owed by Mr. Costeja Gonzalez. He argued that the display of these search results concerning an event that occurred long ago infringed his privacy rights. He argued that the proceedings concerning him were fully resolved several years ago, and thus, the reference to these events was irrelevant.

He requested, that the newspaper be required to remove or alter the pages pertaining to this event so that the personal data relating to him no longer appeared or use certain tools made available by search engines in order to protect the data. He also requested that Google Spain or Google Inc. be required to remove or conceal the personal data relating to him, so that the data no longer appeared in the search results and in the links to La Vanguardia.

The Spanish Data Protection Authority rejected the complaint

against the newspaper, taking the view that the information in question had been lawfully published by it. With respect to the complaint against Google Spain and Google Inc., the Spanish Data Protection Authority requested Google Spain and Google Inc. to take the necessary measures to withdraw the data from their index and to render access to the data impossible in the future.

Google Spain and Google Inc. brought two actions before *Audiencia Nacional*, the National High Court of Spain, claiming that the decision of the Data Protection Authority should be annulled. The Spanish court referred the case to the CJEU.

The CJEU published its decision on Mary 13, 2014.[46] The decision addressed several essential issues, including that:[47]

- Search engines are controllers of personal data. Google can therefore not escape its responsibilities under European law when handling personal data by saying it is a search engine;
- Even if the physical server of a company is located outside Europe, EU rules apply if the company has a branch or a subsidiary in a Member State that promotes the selling of advertising space offered by the company; and
- An individual has the right to request that his or her personal data be removed from accessibility via a search engine.

With respect to the "right to be forgotten," the CJEU ruled that, where information is inaccurate, inadequate, irrelevant or excessive for the purpose of the data processing, individuals have the right to ask search engines to remove links with personal information about them. However, the "right to be forgotten" is not absolute and must be balanced against other fundamental rights, such as the freedom of expression and of the media. The Court found that, in this particular case, the interference with the individual's right to data protection could not be justified merely by the economic interest of the search engine.

---

[46]http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-05/cp140070en.pdf.

[47]CJEU, May 13, 2014, case C-131/12, Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos. Text of the decision, *available at* http://curia.europa.eu/juris/documents.jsf?num=C-131/12.

[B] Aftermath of the CJEU Right to Be Forgotten Ruling

In July 2014, the Data Protection Supervisory Authorities of the EU Member States met to exchange views over the consequences of the CJEU's judgment regarding the right to be forgotten on the Internet.

The objective was to elaborate coordinated and coherent guidelines on the handling of individuals' complaints that may be submitted to the authorities in the case of negative responses from search engines to the request for removal from indexing.[48]

Within the perspective of having a unified European implementation of the CJEU Judgment of May 13, 2014, the Data Protection Supervisory Authorities analyzed the different legal bases allowing individuals—regardless of their nationality, residency and the harm suffered—to invoke the right to request search engines to remove data about them from indexing.

The precise methods of exercising this right to be forgotten and the potential refusals by the search engines to execute this right were also studied. The participants concluded that, in order to effectively exercise this right, individuals must understand when European Union law allows a search engine to reject a request made to exercise their right to be forgotten. The Data Protection Supervisory Authorities addressed the criteria that should be used to balance the right to be forgotten and the public interest in accessing the said information.

The Data Protection Authorities also invited representatives of Google, Microsoft, and Yahoo! to meet in order to discuss the practical implementation of the key principles in the CJEU case in connection with the preparation of guidelines that may be published in the later part of 2014 or early 2015. The guidelines would help ensure a consistent handling of complaints received

[48]Press release, "CJEU's Judgment on the Right to Be Forgotten: the WP 29 Will Meet with Search Engines on July 24th", July 17, 2014, *available at* http://www.cnil.fr/linstitution/actualite/article/article/press-release-wp29-cjeus-judgment-on-the-right-to-be-forgotten-the-wp29-will-meet-with-search/.

from individuals following delisting refusals by search engines.[49]

Many questions were addressed during the meeting and the representatives of the three companies explained their views.[50] Their questions dealt mainly with the modalities of their delisting process (e.g., the scope of application of the ruling, the particular reasons for which there would be a preponderant interest of the general public in having access to the information, the notification of the delisting to third parties, and the justification for refusal). The Data Protection Authorities also asked the search engines to answer some questions in writing by the end of July.

[C] Guidelines on Implementation of the Right to Be Forgotten

In November 2014, the Article 29 Working Party (WP29) published, in its document WP 225, Guidelines on the Implementation of the Court of Justice of the European Union (CJEU) Judgment on Google Spain and Google Inc. v. Agencia Espanola de Proteccion des Datos (AEPD) and Mario Costeja Gonzalez C-131/12 (Guidelines).

These Guidelines provide the Working Party's interpretation of the CJEU's ruling, and identify the criteria that will be used by the EU/EEA Member States Data Protection Authorities when addressing complaints from individuals following a denial of a de-listing request.[51] While a great portion of the Guidelines confirms

---

[49]WP 29 Press Release, July 17, 2014, *available at* http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/20140717_wp29_press_release_meeting_with_search_engines.pdf.

[50]WP 29 Press release, "European DPAs meet with search engines on the 'right to be forgotten,'" July 25, 2014, *available at* http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/20140725_wp29_press_release_right_to_be_forgotten.pdf.

[51]A copy of the guidelines is available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp225_en.pdf.

prior statements made by EU agencies or organizations, some aspects of the Guidelines constitute a significant increase in scope, geography, or consequences from prior positions. Some of the most significant aspects include:

- While the ruling is specifically addressed to search engines, it might apply to other intermediaries;
- The de-listing should affect all domains of a search engine, not just EU based domains;
- Search engines should not comment or indicate on their search results that some listings might be missing as a result of a de-listing request; and
- Search engines should not inform publishers that a posting has been delisted.

[1] Fair Balance Between Fundamental Rights and Interests

In the Guidelines, the WP29 confirms that, as a general rule, the data subject's rights should prevail over the economic interest of the search engine and that of Internet users to have access to personal information through the search engine. The goal here is to address the potential seriousness of the impact that this processing might have on the fundamental rights to privacy and data protection.

However, the WP 29 Guidelines do offer some nuances to this general rule. The WP29 comments that there must be a balance between the relevant rights and interests. In this context, the outcome of any delisting request may depend on the nature and sensitivity of the processed data, and on the interest of the public in having access to that particular information. In particular, the public's interest would be significantly greater if the data subject plays a role in public life. Further, the EU Data Protection Authorities will take into account the public's interest in having access to the information. If the public's interest overrides the rights of the data subject, de-listing will not be considered appropriate.

[2] No Information to Be Deleted from the Original Source

The WP29 points out that the CJEU Judgment makes it clear

that the right granted to individuals only pertains to the results obtained from searches made based on a person's name. It does not require deletion of a link from the indexes of the search engine altogether. The original information should still be accessible using other search terms, or by direct access to the source.

This is important, but might prove cumbersome to implement. When implementing a request for de-listing, the only links that must be removed are those that would appear in response to a search for information regarding a specific person's name. Links to the same article that would be associated with different searches, such as searches focusing on a different topic or different individuals, would survive and remain.

[3] Scope of the Guidelines

The Guidelines allow the CJEU ruling to be expanded to organizations other than search engines. While 'the ruling is specially addressed to generalist search engines,…that does not mean that it cannot be applied to other intermediaries. The rights [to the de-listing] may be exercised whenever the conditions established in the ruling are met."[52] At this point, it is not clear which types organizations may be affected.

[4] Territorial Effect of a De-Listing Provision

The Guidelines add a very important element to the implementation of the "Right to be Forgotten"; this is a much greater geographic scope of the de-listing implementation.

According to the WP29, de-listing decisions must be implemented in such a way that they "guarantee the effective and complete protection of data subjects' rights, and that EU Law cannot be circumvented."[53]

---

[52]Guidelines on the Implementation of the Court of Justice of the European Union (CJEU) Judgment on Google Spain and Google Inc. v. Agencia Espanola de Proteccion des Datos (AEPD) and Mario Costeja Gonzalez C-131/12, pg. 8.

[53]Guidelines on the Implementation of the Court of Justice of the European Union (CJEU) Judgment on Google Spain and Google Inc. v. Agencia Espanola de Proteccion des Datos (AEPD) and Mario Costeja Gonzalez C-131/12, pg. 9.

The WP 29 stresses that limiting de-listing to EU domains on the grounds that users tend to access search engines via their national domains cannot be considered a sufficient means to satisfactorily guarantee the rights of data subjects according to the ruling.

In practice, this means that de-listing should also occur and be effective on all relevant .com and other domains. The WP29 expects that search engines, and other organizations that will receive requests under the "Right to be Forgotten," will implement the de-listing request on all domains on which they operate, and not just on EU or EEA based domains.

[5] Who Is entitled to the Right to Be Forgotten?

The WP29 has indicated that the EU Data Protection Authorities will focus on claims where there is a clear link between the data subject and the EU, such as where the data subject is a citizen or a resident of a EU Member State.

Thus, the ruling and the Guidelines are directed at activities of the EU Data Protection Authorities, and are for the benefit of EU/EEA residents. Individuals residing outside the European Economic Area will not be entitled to seek the same privileges from the EU Data Protection Authorities.

[6] Practical Aspects of De-Listing Requests

The Guidelines address several practical aspects of the delisting request process, such as whether individuals need to contact the original publisher, or how the search engine should communicate its decision. The Guidelines make it clear that individuals are not obliged to contact the original website in order to exercise their rights towards the search engines. Since search engines are deemed data controllers, the applicable national Data Protection Law applies directly to the activity of a search engine.

In addition, the WP29 Guidelines address the role and responsibilities that search engines have in the dissemination and accessibility of information posted on the Internet. In this regard, the Guidelines urge search engines to provide the de-listing criteria they use, and to make more detailed statistics available.

The Guidelines recommend that a search engine that refuses a

de-listing request should provide sufficient explanation to the data subject about the reasons for the refusal. It should also inform data subjects that they can turn to the Data Protection Authority or to a court if they are not satisfied with the answer. If the data subject elects to appeal the decision to the national Data Protection Authority, such explanations would be provided to the Data Protection Authority.

The WP 29 has also commented on the practice adopted by search engines regarding the addition of a notice on some search result pages to indicate that the search results are incomplete because of the application of European data protection laws. The WP 29 comments that this practice would only be acceptable if the information were presented in such a way that users cannot, in any case, conclude that one particular individual has asked for de-listing of results concerning him or her.

Additionally, the WP has commented on the manner in which some search engines have also informed webmasters of the pages that have been affected by de-listing. According to the Guidelines, the only circumstance where this communication would be appropriate is where a search engine would want to contact the original publisher in relation to a particular request before any de-listing decision, in order to obtain additional information for the assessment of the circumstances surrounding that request.

[7] Common Criteria

The second part of the Guidelines contains the list of 13 common criteria that the Data Protection Authorities will apply to handle the complaints filed with their national offices following de-listing refusals. These criteria will be applied on a case-by-case basis and in accordance with the relevant national legislations.

According to the Guidelines, this list of criteria is to be seen as a flexible working tool to help Data Protection Authorities in their analysis of Right to be Forgotten complaints, and during their decision-making process. No single criterion would be determinative. Each of the criteria has to be read in the light of the principles established by the Court and in particular in the light of the public's interest in having access to the information. The specific criteria are:

- Does the search result relate to a natural person, i.e., an individual? And does the search result come up against a search on the data subject's name?
- Does the date subject play a role in public life? Is the data subject a public figure?
- Is the data subject a minor?
- Is the data accurate?
- Is the data relevant and not excessive?
    - Does the data relate to the working life of the data subject?
    - Does the search result link to information that allegedly constitutes hate speech/slander/libel or similar offenses in the area of expression against the complainant?
    - Is it clear that the data reflect and individual's personal opinion or does it appear to be verified fact?
- Is the information sensitive within the meaning of Article 8 of the Directive 95/46/EC?
- Is the data up to date? Is the data being made available for longer than is necessary for the purpose of the processing?
- Is the data processing causing prejudice to the data subject? Does the data have a disproportionately negative privacy impact on the data subject?
- Does the search result link to information that puts the data subject at risk?
- In what context was the information published?
    - Was the content voluntarily made public by the data subject?
    - Was the content intended to be made public? Could the data subject have reasonably known that the content would be made public?
- Was the original content published in the context of journalistic purposes?
- Does the publisher of the data have a legal power or a legal obligation to make the personal data publicly available?

- Does the data relate to a criminal offence?

The Guidelines published by the WP29 are an important document that is likely to evolve in the future. In the meantime, they provide a thoughtful analysis of the different factors and players. They also identify criteria to take into account when examining such requests, and some guidance on how to balance an individual's attempt to forget or mask some of his past or some of his acts, against the (sometimes) legitimate right of some other individuals to have access to this information.