Proposed EU Data Protection Regulation What Companies Need to Know

by Francoise Gilbert, JD, CIPP/US

If the vision of Ms. Reding, Vice-President of the European Commission, as expressed in the January 25, 2012 data protection package is implemented in a form substantially similar to that which was presented in the package, by 2015, the European Union will be operating under a single data protection law that applies directly to all entities and individuals in the Member States and will have removed much of the administrative burden that are currently costing billions of Euros to companies. The saving would allow companies to reinvest in more meaningful, efficient, data protection practices that are better adapted to the uses of personal data, the new technologies and the 21st century way of life.

The series of legislative texts and documents that were published on January 25, 2012 by the European Commission are intended to redefine the legal framework for the protection of personal data throughout the European Economic Area. Ms. Reding's vision is to have a Regulation address the general privacy issues, and a Directive address the special issues associated with criminal investigations.

The publication of these drafts signal a very important shift in the way data protection will be handled in the future throughout the European Union. The proposed rules would create more obligations for companies and more rights for individuals, while some of the current administrative burdens and complexities would be removed. This is consistent with the plan of action that was presented in late 2010 in Communication 609. What is new, and a paradigm shift, is that there will be **one single data protection law throughout the European Union**, and companies will not longer have to suffer from the fragmentation resulting from the fact that the 27 Member States interpreted and implemented differently the principles set forth in

About the IT Law Group

The IT Law Group (www.itlawgroup.com) assists clients in complying with data privacy and security laws in the United States and around the globe; and in negotiating and structuring large-scale cloud computing arrangements. Our practice areas encompass a wide range of matters from behavioral targeting to mobile marketing, and crossborder transfers to cloud computing.

About Francoise Gilbert

Francoise Gilbert, JD, CIPP/US, focuses her legal practice on information privacy and security, cloud computing, and data governance.

She was voted one of the country's top legal advisors on privacy matters in a recent industry survey and, for several years, has been recognized by Chambers, Best Lawyers, *and* Ethisphere *as a leading lawyer in the field of information privacy and*

security.

Gilbert is the author and editor of the two-volume treatise **Global Privacy & Security Law** (2,900 pages; Aspen Publishers, Wolters Kluwer Law and Business) *(www.globalprivacybook.com), which analyzes the data protection laws of 65 countries on all continents.*

She is the managing attorney of the **IT Law Group** *(www.itlawgroup.com). In addition, she serves as the general counsel of the Cloud Security Alliance.*

She also keeps a blog on domestic and international data privacy and security issues (www.francoisegilbert.com) and writes a monthly column for TechTarget on cloud computing legal issues (http://searchcloudsecurity.techtarget.com/contributor/Francoise-Gilbert)

Contact Us

For further information, please contact:

Directive 95/46/EC.

A single set of rules on data protection, valid across the EU would make it easier for companies to know the rules. Unnecessary administrative burdens, such as notification requirements for companies, would be removed. Instead, the proposed Regulation provides for increased responsibility and accountability for those processing personal data. In the new regime, organizations would only have to deal with a single national data protection authority in the EU country where they have their main establishment. Likewise, people would be able to refer to the data protection authority in their country, even when their data are processed by a company based outside the EU.

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

The Foundation Documents

The proposed data protection package contains two important legislative texts:

- A proposed Regulation: *General Data Protection Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, which will supersede Directive 95/46/EC; and
- A proposed Directive: *Police and Criminal Justice Data Protection Directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection, or*

Francoise Gilbert
+1 650-804-1235
fgilbert@itlawgroup.com

Legal Notices

prosecution of criminal offenses or the execution of criminal penalties, and the free movement of such data.

The draft Regulation and draft Directive will now be discussed by the European Parliament and EU Member States meeting in the Council of Ministers. Thus, there will be more opportunities for discussion, changes, and modifications of the current provisions, and there is currently no certainty that the provisions as stated in the January 25, 2012 draft will remain.

However, given the energy, speed, and determination with which the reform of the EU data protection regime has been handled, it is likely that a final vote will take place sooner than later. Once in their final form and formally adopted by the European Parliament, the rules are expected to take effect two years later. Thus, it is likely that, by the end of 2014, or early 2015, the European Economic Area will be subject to a new, improved, but stricter data protection regime.

This article discusses only the Proposed Regulation.

Regulation v. Directive

The European Union is over 50 years old. For a long time, the 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 implementing on a piecemeal basis the principles of numerous directives, with each Member State, in fact, retaining a lot of independence and autonomy. While this strategy allowed to slowly create 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 but also their own personality. A difficult setting for companies operating in 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. It marked a very important step in the evolution of the Union, creating deep changes in its rules of operation, 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 towards more cohesion, more consistency, and more unity.

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 the protection of personal data in the European Union in connection with the processing of these data by companies and government agencies in their day-to-day operations. Due to the legal nature of a regulation under EU law, the proposed data protection Regulation will establish a single rule that applies directly and uniformly.

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.

EU directives, on the other end, are used to bring different national laws in-line with each other. They 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 - Directive 96/45/EC, Directive 2002/558/EC (as amended) and Directive 2006/2006/24/EC - has proved to be very cumbersome due to the significant discrepancies between the interpretations or implementations of the directive that were made in the various Member State data protection laws. There is currently a patchwork of 27 rules in 27 countries. This fragmentation creates a significant burden on businesses which are forced to act as chameleon, and adapt to the different privacy rules of the countries in which they operate.

Conversely, a regulation is directly applicable, as is, in the Member

States. By adopting a Regulation for data protection matters, the EU will equip each of its Member States with the same legal instrument that applies uniformly to all companies, all organizations, and all individuals. The choice of a regulation for the new general regime for personal data protection should provide greater legal certainty by introducing a harmonized set of core rules that will be the same in each Member State. Of course, each country's government agencies and judicial system are still likely to have their own interpretation of the same text, but the discrepancies between these interpretations should be less significant than those that are currently found among the Member State data protection laws.

Overview of the Draft Regulation

The 119-page draft Regulation lays out the proposed new rules. Among the most significant changes, the Proposed Regulation would shift the consent requirement to that of 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 information of children, the use of binding corporate rules, the special status of data regarding health, and the requirement for a data protection officer. It would require companies to conduct privacy impact assessments, to implement "Privacy by Design" rules, and to ensure "Privacy by Default" in their application. Individuals would have greater rights, such as the "Right to be Forgotten" and the "Right to Data Portability." Some of the key components of the Proposed Regulation are discussed below.

- New, Expanded Data Protection Principles

Articles 5 through 10 would incorporate the general principles governing personal data processing that were laid out in Article 6 of Directive 95/46/EC and add new elements such as: transparency principle, comprehensive responsibility and liability of the controller, and clarification of the data minimization principle.

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

website. Under the new regime, when consent is the basis for the legitimacy of the processing, it will have to be "specific, informed, and explicit." 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.

- Special Categories of Processing

The rules that apply to special categories of processing would be found in Articles 80 through 85. The special categories would include processing of personal data for:

- Journalistic purposes;
- Health purposes;
- Use in the employment context;
- Historical, statistical or scientific purposes;
- Use by individuals bound by a duty of professional secrecy;
- Public interest.

There are also provisions to protect the rights of a child. A "child" is currently defined as an individual under 13 (Article 8). In addition, the definition of "sensitive data" would be expanded to include genetic data and criminal convictions or related security measures. (Article 9).

- Transparency and Better Communications

Article 11 of the proposed Regulation would introduce the obligation for transparent and easily accessible and understandable information, while Article 12 would require the controller to provide procedures and a mechanism for exercising the data subject's rights, including means for electronic requests, requiring that response to the data subject's request be made within a defined deadline, and the motivation of refusals. Companies will welcome the fact that the rule for handling requests for access or deletion will 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 two months to respond.

- Rights of the Data Subjects

Articles 14 through 20 would define the rights of the data subjects. 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. The right to be forgotten includes the right to obtain erasure of any public Internet link to, copy of, or replication of the personal data relating to the data subject contained in any publicly available communication service. It also integrates the right to have the processing restricted in certain cases.

Article 18 would introduce the data subject's right to data portability, that is, to transfer data from one automated processing system to, and into, another, without being prevented from doing so by the controller. As a precondition, it provides the right to obtain from the controller those data in a commonly used format. The right to object to the processing of personal data would be supplemented by a right not to be subject to measures based on profiling.

The "right to be forgotten" and the "right to portability" reflect the pressure of the current times, and respond to the needs of customers of social networks who have found, 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 expected, and that the service provider would resist a user's attempt to move to another service.

- 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. Article 22 addresses the accountability of the controllers. These would include for example, the obligation to keep documents, to implement data security measures, and to designate a data protection officer. Article 23 would set out the obligations of the controller to ensure data protection by design and by default.

Articles 24 and 25 address some of the issues raised by outsourcing,

offshoring and cloud computing. While these provisions do not indicate whether 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 responsibility for compliance with the Proposed 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 and that direct data processing activities at EU residents, or monitor their behavior, to appoint a designated representative in the European Union.

- Supervision of Data Controllers or Processors

Article 28 would introduce the obligation for controllers and processors to maintain documentation of the processing operations under their responsibility, instead of a general notification to the data protection supervisory authority, as is currently the case under Articles 18 and 19 of Directive 95/46/EC. This provision reflects one of the new guiding principles in the EU Data Protection reform: that of accountability. In exchange for removing the cumbersome requirement for notification of the data controllers' personal data handling practices, the new framework require that data controllers be "accountable." They must create their own structures, and document them thoroughly, must be prepared to respond to any inquiry from the Data Protection Authority and to promptly produce the set of rules with which they have committed to comply.

Article 28 identifies a long list of documents that would have to be created and maintained by data controllers and data processors. This information is somewhat similar to the information that is currently provided in notifications to the data protection authorities—for example, the categories of data and data subjects affected, or the categories of recipients. There are 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.

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 the supervision of the processing activities of that processor or controller in all Member States under the mutual assistance and cooperation provisions that are set forth in the Proposed Regulation.

- Data Security

Articles 30 through 32 focus on the security of the personal data. In addition to the security requirements already found in Article 17 of Directive 95/46/EC and extending these obligations to the data processors, the Proposed Regulation introduces an obligation to provide notification of personal data breaches. In case of a breach of security, a data controller would be required to inform the supervisory authority within 24 hours, if feasible. In addition, if the breach is "likely to adversely affect the protection of the personal data or the privacy of the data subject," the data controller will be required to notify the data subjects, without undue delay, after it has notified the supervisory authority of the breach.

- Data Protection Impact Assessment

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.

- Data Protection Officer

Articles 35 through 37 would require the appointment of a data protection officer for the public sector, and, in the private sector, for large enterprises or where the core activities of the controller or processor consist of processing operations that require regular and systematic monitoring. Under the current data protection regime, several EU Member States, such as Germany, require organizations to

hire a Data Protection Officer, who is responsible for the company's compliance with the national data protection. Article 36 identifies the roles and responsibilities of the data protection officer and Article 37 defines the core tasks of the data protection officer.

- Crossborder Data Transfers

Articles 40 through 45 would define the conditions of, and restrictions to, data transfers to third countries or international organizations, including onward transfers. For transfers to third countries that have not been deemed to provide "adequate protection," Article 42 would require that the data controller or data 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 (currently they are only accepted in about 17 Member States);
- The use of contractual clauses is subject to prior authorization by supervisory authorities.

Binding corporate rules would take a prominent place in the Proposed Regulation. Their required content is outlined in Article 43. Article 44 spells out and clarifies the derogations for a data transfer, based on the existing provisions of Article 26 of Directive 95/46/EC. In addition, a data transfer may, under limited circumstances, be justified on a legitimate interest of the controller or processor, but only after having assessed and documented the circumstances of the proposed transfer.

- European Data Protection Board

The "European Data Protection Board" would be the new name for the "Article 29 Working Party." Like its predecessor, the new Board will consist of the European Data Protection Supervisor and the heads of the supervisory authority of each Member State. Articles 65 and 66 clarify the independence of the European Data Protection Board and

describe its role and responsibilities.

- Remedies and Sanctions

Articles 73 through 79 would address remedies, liability, and sanctions. Article 73 would grant data subjects the right to lodge a complaint with a supervisory authority (which is similar to the right under Article 28 of Directive 95/46/EC). It also would allow consumer organizations and similar associations to file complaints on behalf of a data subject or, in case of a personal data breach, on their own behalf.

Article 75 would grant individuals a private right of action. It would grant individuals the right to seek a judicial remedy against a controller or processor in a court of the Member State where the defendant is established or where the data subject is residing. Articles 78 and 79 would require Member States to lay down rules on penalties, to sanction infringements of the Proposed Regulation, and to ensure their implementation. In addition, each supervisory authority must sanction administrative offenses and impose fines.

The Proposed Regulation introduces 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. 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.

Conclusion

The terms of the Proposed Regulation are not really a surprise. For several months, Viviane Reding, Vice-President of the European Commission, and other representatives of the European Union have provided numerous descriptions of their vision for the new regime, including through a draft of the documents published in December 2011, which differs slightly from the January 25, 2012 version. It is nevertheless exciting to see, at long last, the materialization of these

descriptions, outlines, and wish lists.

Altogether, if the current provisions subsist in the final draft, the new Regulation will increase the rights of the individuals and the powers of the supervisory authorities. While the Regulation would create additional obligations and accountability requirements for organizations, the adoption of a single rule throughout the European Union would help simplify the information governance, procedures, record keeping, and other requirements for companies.

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

* * * * * * *

Useful Links

- Data Protection Reform website

http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm

- January 25, 2012 Communication

http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_9_en.pdf

- January 25, 2012 draft of the Regulation

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

- January 25, 2012 draft of the Directive

http://ec.europa.eu/justice/data-

protection/document/review2012/com_2012_10_en.pdf

- November 2010 Communication. Overview and Comments

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

- Treaty of Lisbon (2009)

http://www.consilium.europa.eu/treaty-of-lisbon?lang=en

- Directive 95/46/EC

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML