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

by Francoise Gilbert, JD, CIPP/US

The comprehensive proposed data protection package that the European Commission unveiled on January 25, 2012 provides a sneak preview of the plans for the reform of the data protection rules in the European Union. The new data protection framework would be based on two documents: a Regulation, which would address the general privacy issues, and a Directive, which would address the unique issues associated with criminal investigations. The proposed legislative texts are intended to redefine the legal framework for the protection of personal data throughout the European Economic Area.

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

The vision revealed in the documents published on January 25, 2012 is generally consistent with the plan of action that was presented in late 2010. What is new, or was not clearly specified in 2010, is the shift to a single law that would be common to all of the Member States. If the proposed texts are adopted, there will be one single data protection law throughout the European Union. Companies would no longer have to suffer from the fragmentation resulting from the significant discrepancies in the manner in which the 27 Member States interpreted and implemented the principles set forth in Directive 95/46/EC to create 27 different sets of national laws.

A single set of rules on data protection, valid across the EU,
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) and 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).

Contact Us

For further information, please contact:

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

Legal Notices

© 2012 IT Law Group – All rights reserved

This publication is issued

The Foundation Documents

The proposed data protection package contains two important legislative texts and an introductory document in the form of a Communication, which provides background on the origin of the new regime. The proposed reform would create more obligations for companies and more rights for individuals, while some of the administrative burdens that currently cost billions of Euros to companies will have been removed. However, numerous additional requirements would come instead. While the new data protection regime would reduce red tape, it would require companies to be more accountable, to have in place written procedures and processes that they actually use, and to be able to show that they do comply with the applicable legal requirements. They would be responsible for conducting privacy impact assessments in some circumstances, to comply with individual requests to exercise their “right to be forgotten,” and to notify data protection authorities and individuals in the event of a breach of security.

U.S. 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 to be created accordingly. The development of these new structures will require significant investment and resources. IT and IS departments in companies will need to obtain greater, more significant budgets in order to finance the staff, training, policies, procedures and technologies that will be needed to implement the new provisions.
periodically to keep clients of the IT Law Group and other interested parties informed of current legal developments that may affect, or be of interest to them. It is designed to give general information on the developments actually covered. It is not intended to be a comprehensive summary of recent developments in the law, or treat exhaustively the subjects covered. The comments contained herein do not constitute legal opinion and should not be regarded as a substitute for legal advice.

and the development of the two proposed legislative texts. These two proposed legislative texts include:

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

The 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. Consequently, there is currently no certainty that the provisions as stated in the January 25, 2012 draft will remain.

Given the energy, speed, and determination with which the reform of the EU data protection regime has been handled, however, 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. In the first part, after providing the necessary historical and legal background to understand the genesis and nature of the proposed document, we analyze and discuss the provisions of the January 25, 2012 draft of the Proposed Regulations. Then we address whether the initial goal of uniformity and consistency might not be derailed by several provisions that grant Member States extensive powers to carve out, make restrictions or add new provisions to the common
Background; EU Law Basics

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

Historical Milestones

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. When implementing the directives, each Member State, in fact, retained – or elected to take – a lot of independence and autonomy. 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. These inconsistencies and discrepancies created 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 critical 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. Shortly thereafter, in November 2010, taking advantage of the new structure and new expanded powers, the European Commission published a document that outlined its plans to reform the data protection regime in the European Union to conform to the new structures created by the Treaty of Lisbon. Most of the key elements described in the November 2010 document that presented the blue print for the reform are found in the proposed legislative text published in January 2012.
Regulation v. Directive

With this background in mind, it is logical that the European Commission found that a “regulation,” as opposed to a “directive,” was the most appropriate legal instrument to define the new framework for regulating the processing of personal data by companies and government agencies in their day-to-day operations. Due to the legal nature of a regulation under EU law, the proposed data protection Regulation is the best medium for establishing 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 – 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, the 27 Member States created a patchwork of 27 rules with different structures, different wording, and different basic rules. 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.

Conversely, a regulation is directly applicable, as is, in the Member States. By adopting a Regulation for data protection
matters, the EU Commission intends to equip each of its Member States with the same basic legal instrument that applies uniformly 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.

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

The United States may be an example of this constant quagmire. The United States has numerous federal laws that 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 the same laws continue to be interpreted differently throughout the U.S. States and territories. 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, it would be very risky to act as if there were total uniformity.

**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 change the consent process 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 use of binding corporate rules, the special status of health information, and the requirement for a data protection officer for most corporations and government agencies. It would also 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 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. The seven basic principles relating to data processing would require that the personal data be:

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

**Specific, Informed and Explicit Consent**

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. 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 consent is the basis for the legitimacy of the processing, it 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 cookies are treated under the 2009 amendments to Directive 2002/58/EC. As a result of these amendments many of the EU Member States have modified their national laws to require that the user’s specific (opt-in) consent be obtained before cookies, other than technical cookies, can be sent to the user’s computer.

**Special Categories of Processing**

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

**Protection of Children Under 13**

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

**Expanded Definition of Sensitive Data**

The definition of “sensitive data” would be expanded to include genetic data and criminal convictions or related security measures (Article 9). The notion of what constitutes “sensitive data” would continue to be significantly different from that of the United States. In the United States, data that are generally identified as “sensitive” tend to be those that would result in identity theft in case of a loss or breach of security; for example, credit card or drivers 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 (for example, information about health or sexual preference) or that may cause discrimination or retaliation (for example, information about religion or trade union membership).

**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
- 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.
Crossborder Data Transfers

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. There may be some relief on these issues. One of the key aspects of the plan is to put in place a “one-stop-shop” approach, remove the discrepancies in the regimes for crossborder data transfers, and to validate the use of binding corporate rules.

In the new 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;

- The use of contractual clauses other than the standard clauses would be subject to prior authorization by the 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. 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 provides for international cooperation mechanisms for the protection of personal data between the European Commission and the supervisory authority of third countries. It should be noted that Article 42 of the prior draft of the Regulation (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.

**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.

✅ **Accountability**

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

Under the Regulation, accountability would require that the data controller 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:
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.

**Documentation Requirements; Supervision by Data Protection Authority**

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.

This removal of the notification requirement reflects one of the new guiding principles in the EU Data Protection reform: that of accountability. In exchange for abolishing the cumbersome notification requirement, the new Regulation would require that data controllers and data processors to be “accountable.” They would have to create their own structures, and document them thoroughly. They would have to 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. The information required 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, 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.

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 mutual assistance and cooperation provisions that are set forth in the Proposed Regulation.

**Allocation of Responsibilities among Joint Controllers**

Articles 24 and 25 address some of the issues raised by outsourcing, offshoring and cloud computing. While these provisions do not clearly indicate whether or when outsourcers are joint data controllers, they acknowledge the fact that there may be more than one data controller. Under Article 24, joint data controllers would be required to determine their own allocation of 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, when their data processing activities are subject to the Regulation, to appoint a designated representative in the European Union.

**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.

**Special Rules for Data Processors and Subcontractors**

Article 27, which is based on Article 16 of Directive 95/46/EC, would generally follow the existing provisions to define the rules for processing under the authority of the data controller. As is currently 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 chose to move a data center or disaster recovery center to a different location without consulting with the client, would it become a joint-controller if the provisions of this new Article 26 were applied?

**Security of Personal Information**

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

✓ **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” (Article 4(9)).

In case of a breach of security, a data controller would be required to inform the supervisory authority within 24 hours, if feasible (Article 31). A data processor that is the victim of a breach would also be required to alert and inform the data controller immediately after establishing that a breach of security occurred.

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 would be required to notify the data subjects, without undue delay, after it has notified the supervisory authority of the breach (Article 32). 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 (Preamble, Recital 67).

---

**Additional Requirements**

✓ **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.

**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.

**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”.

**Transparency and Better Communications**

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

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

**Right of Information**

The right of information would be expanded from the current Articles 10 and 11 of Directive 95/46/EC, to provide additional information to the data subject than is currently required. For example, individuals would have to be informed of the length of the period during which the data controller intends to hold their data. They would also have to be informed of their right to lodge a complaint, of the proposed crossborder transfers of personal data, and of the source from which the data are originating (Article 14).

**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 (Article 15).
Right of Rectification

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

Right to Object to the Processing

Article 14 of Directive 95/46/EC contained a right to object to the processing of personal data. This right would be provided by Article 19 of the 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.

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 modifications and additional safeguards.

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 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.

Right to Data Portability

Article 18 would introduce the data subject’s right to “data portability”, that is, the right to transfer data from one automated
processing system to, 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 Regulation is technology neutral. It does not explain how the copy could be created and what format can be used to ensure that the file can be uploaded and read by a different social media platform.

The “right to be forgotten” and the “right to portability” reflect the pressure of the current times. There have been numerous reports of the unexpected consequence of the use of social media. 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 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 back up media, or duplicated on a host site for disaster recovery and business continuity purposes. On the other hand, content that was intentionally provided to subcontractors, service providers or co-marketers might be more easily traceable, for example, if the company keeps a log of its data transfers.

Complaints, Judicial Remedies, Class Actions

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

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

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 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.

Class Actions

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

These additions are very important. They would open the door to actions similar to a class action suit, a form of action that is currently seldom used in the European Union, but with which U.S. companies 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 attorneys fees. The injured parties or the parties directly affected by an incident may only receive a very small amount of money compared to the large settlement amount.

**Damages and Sanctions**

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

**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. When more than one entity is involved in the processing, the controllers and processors would be held jointly and severally liable for the entire amount of the damages.

**Penalties and Sanctions**

Articles 78 and 79 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 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 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 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 .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 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 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 Key Players

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

**Data Protection Supervisory Authorities**

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

- **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 (Article 46) and to implement the relevant case law (Articles 47, 48).

  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 (Article 52), and preparing annual reports (Article 54). 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.

- 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 Member States. In some cases, unity and consistency may be obtained through opinions of the European Data Protection Board, discussed below (Article 58). There are also provisions giving power to the European Commission to intervene (Article 59 to 63).

✓ 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 (Article 64). The
composition of the group would be slightly different from that of the Article 29 Working Party. The EU Commission would 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.

Possible Divergence Among the Member States?

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

✓ Ability to Create Additional Restrictions

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

- Public security;
- The prevention, investigation, detection and prosecution of criminal offenses;
- Important economic or financial interests of the 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 of prosecutions of breaches of ethics for regulated professions;
- The monitoring, inspection or regulatory function connected with the above; or
- The protection of the data subjects or the rights and freedom of others.
While this provision is substantially similar to Article 13 of Directive 95/46/EC, it should be expected that Member States might be tempted to use it in order to regain some of the freedoms that they may have lost otherwise as a result of the adoption of the Regulation.

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

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

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

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

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

✓ **Privacy and Freedom of Expression**

In addition to the provisions of Article 21 of the Proposed Regulation, numerous other provisions could allow Member States to enact their own laws. For example, traditionally there has been an inconsistency between the right of privacy and the freedom of expression. This discrepancy would subsist, and States would have the freedom to limit privacy rights to address freedom of information issues. 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 (Article 80). The scope of the power of the Member State 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.

✓ **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 (Article 81), the protection of employee personal data in the employment context (Article 82), rules regarding interaction with professionals having an obligation of secrecy (Article 84) and the collection of personal data by churches and religious associations (Article 85).

✓ **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.
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.

Conclusion

The terms of the Proposed Regulation are not a major surprise. For several months, Viviane Reding, Vice-President of the European Commission, and other representatives of the European Union have provided numerous descriptions of their vision for the new regime, 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 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 suggested by the Regulation.

Finally, it should also be remembered that Directive 95/46/EC has been a significant driving force in the adoption of data protection laws throughout the world. In addition to the 30 members of the European Economic Area, numerous other countries, such as Switzerland, Peru, Uruguay, Morocco, Tunisia, or the Dubai Emirate (in the Dubai International Financial District) have adopted data protection laws that follow closely the terms of Directive 95/46/EC. 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
- January 25, 2012 Communication
- January 25, 2012 draft of the Regulation
- January 25, 2012 draft of the Directive
- November 2010 Communication. Overview and Comments
- Treaty of Lisbon (2009)
- Directive 95/46/EC