wiley

NEWSLETTER

Proposed New European Union Data Regulation Raises Significant Issues for U.S. Businesses

February 2012

On January 25, the European Commission (EC) released the final text of its long-awaited proposed new Data Protection Regulation, which would replace the 1995 European Union (EU) Data Protection Directive that currently governs the collection, use and transfer of personal data within and beyond the EU. The EU also issued a Directive regarding the protection of personal data in the course of the investigation and prosecution of criminal offenses.

The new European General Data Protection Regulation, if adopted as proposed, would apply privacy rules that in some cases simplify, and in other cases expand, current EU law. The EU privacy rules are substantially different than those imposed by U.S. law and will present significant compliance challenges for U.S. companies doing business in Europe—including those transacting with European nationals solely through the Internet without a physical presence in Europe. The new regulations could take effect as early as 2014; however, experts believe that it will be at least 2015 before the new rules become fully effective.

Background and Objectives

The result of a revision process that began in November 2010, the proposed Regulation would replace the 1995 EU Data Protection Directive—a framework that guided EU member states as to privacy, yet granted individual nations broad discretion to implement their own laws. While the Regulation is more moderate in some respects than an earlier draft leaked during the process, for the most part, it is consistent with the leaked draft and is generally more restrictive than

Authors

Brandon J. Moss
Partner
202.719.7554
bmoss@wiley.law

current law.

Proponents of the proposed Regulation proclaim that it is an attempt to promote consumer confidence and streamline commerce by increasing protections of individuals' data while reducing red tape for business and guaranteeing the free circulation of data within the EU. In a release, EU Justice Commissioner Vivian Reding, the chair of the Article 29 Working Party and primary drafter of the proposed Regulation, said:

My proposals will help build trust in online services because people will be better informed about their rights and in more control of their information. The reform will accomplish this while making life easier and less costly for businesses. A strong, clear and uniform legal framework at EU level will help to unleash the potential of the Digital Single Market and foster economic growth, innovation and job creation.

The proposed Regulation would, to a material degree, simplify operations in Europe, because it would have the status of a "Regulation" instead of the current privacy "Directive." As a Regulation, the rules would take effect throughout the EU without requiring the individual Member States to enact implementing legislation, as is the case under the current Directive. This would address a problem the EU has experienced with Member States moving slowly to implement the current Data Privacy Directive, or doing so in inconsistent ways.

In addition to creating a single set of rules throughout the EU, the Regulation would eliminate the obligation for companies to file notifications of their data protection practices with national data protection authorities. Instead, businesses could deal with the Data Protection Authority in only one country—the one of its principal place of business in the EU—rather than separately with DPAs in each country.

On the other hand, the proposed Regulation would impose a number of burdens on businesses operating in Europe. Importantly, the Regulation as currently drafted would create jurisdiction over American-based organizations doing business in Europe, whether as government contractors, consumer-facing businesses or Internet-based businesses (including providers of cloud computing). The Regulation will be especially tough on U.S. businesses, because the EU proposals flow logically from EU concepts of personal data—concepts that are often quite contrary to how U.S. companies view consumer data.

Proposal Nuts and Bolts

First, wherever EU law requires "consent" for the collection, use or transfer of personal data, the proposed Regulation requires that the consent must be "explicit." What that means in practice can vary. However, early indications are that the rule would be made particularly strenuous by the Regulation's broad definition of personal data as "any information relating to an individual, whether it relates to his or her private, professional or public life." This could include, for example, posts to social networking websites and computer IP addresses, as well as photographs, email addresses and financial data.

Second, the final proposed Regulation reduces the potential maximum fine for businesses, from five percent of worldwide "turnover" or gross income mentioned in the earlier leaked draft, to two percent. Still, for a large company, such a fine could be enormous.

Third, the final proposal contains a provision requiring companies in certain cases to provide data breach notification to relevant data protection authorities and individuals within 24 hours of the discovery of a breach "if feasible."

Fourth, if passed, the Regulation would create a "right to be forgotten," which appears intended to allow individuals to demand the removal of personal data from the Internet, including social networks, and other business records unless there is a valid business reason to retain it. Using such personal data for future marketing would likely not be regarded as a valid reason. Notably, news organizations would not have to delete references to persons from published newspapers or past broadcasts.

Fifth, the proposed regulation creates a "right of portability" for all EU citizens. Pursuant to this newly proposed right, websites must allow consumers to transport their information from one site to another site. For example, each social networking site must allow its users to transfer all materials the user chooses to post on that site to another social networking site at any given time.

Sixth, companies with more than 250 employees would be required to designate a data protection officer. These companies would also have to conduct Privacy Impact Assessments and make use of the concept of "Privacy By Design" (the concept that privacy assurances should be a default mode of operation).

Seventh, the Regulation would require that companies have a "transparent and easily accessible" policy for all personal data processing activities. Moreover, companies must provide information about such data processing policies to consumers at the point of data capture. Relatedly, companies must document all processing operations involving personal data.

Finally, and quite possibly most noteworthy for U.S. companies, the Regulation would apply to "personal data handled abroad by companies that are active in the EU market and offer their services to EU citizens." This would apply the EU rules to American companies that offer goods or services to data subjects in the EU or monitor data subjects' behavior.

In summary, if adopted, the Regulation would place a much larger burden on U.S. companies than either U.S. law or the current 1995 Directive. New items of particular importance to all American businesses include the duty to have a representative in the EU, the "right to be forgotten," the right of "data portability" and potentially severe fines for violating regulatory requirements. Additionally, it is worth noting that, while big businesses may fear the severe fines proposed, the Regulation's real burden may be felt disproportionally by small and medium companies who would have to hire Data Protection Officers and possibly re-configure their entire world-wide platforms to comply with European law.

"Safe Harbor" and BCR Impacts

The regulation would not directly abrogate the "safe harbor" agreement between the EU and the U.S. Department of Commerce that currently allows data transfers from the EU to the U.S. However, it seems likely that the agreement and its requirements might be subject to some further negotiation at some point if the Regulation were adopted.

Optimistically, the EC asserts that the new rules will simplify and streamline the existing Binding Corporate Rules (BCR) process—a process that is presently so complex and expensive that only a few select large businesses have taken advantage of the BCR option. To some extent, the Commission has succeeded as at least BCRs are now detailed in a legal text. However, for the most part, the traditional challenges and costs associated with the process remain. In fact, to the extent the BCR requirements now seem to be less stringent than past requirements, which sometimes far exceeded baseline requirements under the Directive and various countries' implementing laws, it may be only because the BCR requirements are more in line with the new proposed Regulation's strict requirements. Thus, as it remains to be seen whether or not the mere incorporation of BCRs in the Regulation will simplify the existing BCR process, small and medium companies may have to wait to see how the "new" regime will play out before attempting to take advantage of this avenue when transferring data to third countries.

What Happens Next?

As a matter of process, the proposal will now be reviewed by the European Parliament and the European Council. This could take two to three years, and the proposal could be changed significantly in the course of this process, much like proposed legislation in the U.S. Congress. In particular, preliminary indications are that the proposed Regulation may face resistance by France, and perhaps other countries, and the approval process is likely to be the focus of a fierce lobbying war. Additional time may elapse after its adoption before it takes effect.

That said, it would be wise for companies making long-term plans regarding data management polices to keep an eye on Brussels as the European Parliament begins to take up this important proposal.