Keeping Pace With EU Data Privacy Law Overhaul

Law360, New York (February 22, 2012, 1:19 PM ET) -- The European Union has unveiled plans for sweeping changes to its outdated data protection laws that will have significant implications for companies — both inside and outside the EU — that handle the data of EU citizens, and may subject those that fail to comply with severe fines of up to 2 percent of annual global income.

According to the Jan. 25, 2012, statement from the European Commission announcing the reforms, the proposed General Data Protection Regulation — one component of the package of reform measures — is intended to update and modernize the 1995 Data Protection Directive to strengthen online privacy rights, as well as make more consistent the enforcement of data protection requirements across all of the EU member states.

While the proposed regulation is also intended to reduce both the administrative burdens and the cost of compliance for companies subject to its requirements, the resulting overhaul of the current EU privacy framework may impact so fundamentally the way that companies conduct their business and expose them to such large penalties that compliance with the new requirements may require companies to undertake a comprehensive redesign of their privacy and data security policies and procedures across all operations, both inside and outside the EU, as well as provide extensive employee training.

A Single Regime for Personal Data Applicable in All 27 EU Member States

Because the new requirements for collecting, storing and using personal data are embodied in a regulation, they would apply in all 27 EU member states, in their entirety, as written. In contrast, the previous privacy principles were in the form of a directive, which is binding on the member states only with respect to the outcome to be achieved and leaves open to each national authority how it chooses to achieve it. The proposed regulation would replace the current, fragmented system of varied privacy standards individually implemented by member states to comply with the current directive.

In addition, as explained in a memo on the proposed amendments, a company would be under the jurisdiction of only one Data Protection Authority (DPA) — the one in the member state in which the company has its main establishment. Increased coordination between DPAs in all the member states would work to ensure that the new EU data protection rules are applied and enforced consistently across all member states — and across all operations of a company, even if they are located in more than one member state.

The proposed regulation does not guarantee that enforcement of the new privacy requirements will be 100-percent consistent across the EU, however, since member states may have to enact or amend national legislation to bring them in line with the regulation — and the regulation is still subject to some interpretation by the authorities in each member state.

While compliance with a single set of regulations — rather than 27 — and dealing with the determinations of a single DPA may be simpler and perhaps less costly, the new uniform requirements overall are stricter and more onerous — significantly so when compared to existing requirements in member states with comparatively more lenient privacy laws (such as the U.K.).

Compliance by U.S. and Non-EU-Based Companies

The proposed regulation would apply to U.S. and non-EU-based companies that offer their goods and services to, or that monitor or track the online behavior of, EU citizens. According to the explanatory memo, the intent of the proposed regulation is to protect individuals' rights to privacy relating to their personal data, and increasingly, the collection and processing of data takes place outside of the EU.

For example, companies that collect personal data in the course of transactions with EU citizens, or that track their online behavior of EU citizens for the purposes of creating profiles of personal preferences, would be required to comply with the new privacy requirements.

Additional Rights and Strengthened Control Over Personal Data by Individuals

The proposed regulation aims to give individuals more control over the collection, storage and use of their personal data — a broad category of information related to individuals' personal, professional or public lives, including identifying information, such as name, address or email, financial and medical information, and computer-related information (IP addresses and online identifiers in some circumstances), as well as photos and posts on social networking sites.

The regulation requires, among other things, that where consent to collection and processing of data is required, that the consent is explicit — "based either on a statement or on a clear affirmative action by the person concerned and is freely given." The consent must be specific to the data processing, not part of a general consent.

The regulation also provides for "privacy by default" — a company's online default settings must be those that provide the most privacy for individuals — and also requires transparent, easily accessible policies relating to the processing of personal data and to the exercise of individuals' rights. For many companies engaged in e-commerce, these new requirements may necessitate implementing new or additional online devices to gain consent, changing default settings, and revising — and rewriting — privacy policies.

Companies also would be required to afford Individuals a "right to be forgotten." While the oft-used example for illustrating the need for the right to be forgotten is the social networking site that retains personal information after an individual stops using the service, all data controllers would be required to delete an individual's personal data if that person explicitly requests deletion and the data controller has no other legitimate reason to retain it.

The right to be forgotten also requires companies to minimize the volume of users' personal data that they collect and process, delete personal data when an individual withdraws consent or when the consented-to retention period expires, as well as when the personal data is no longer necessary for the purposes for which it was collected. These affirmative obligations to afford individuals the right to have their data deleted may require companies to implement new or additional data retention policies and procedures to ensure compliance.

The right also requires a data controller who has authorized the third-party publication of personal information to inform those third parties whenever an individual requests the deletion of their data. Under the regulation as proposed, companies must advise third parties that the individual requests personal information be erased or rendered inaccessible, but do not have an affirmative obligation to ensure that the third party complies.

In addition to the right to be forgotten, data controllers must also afford individuals the right to "data portability" — the right to obtain a copy of their own stored data and the ability to transfer personal data more easily from one service provider to another, without hindrance.

Increased Data Security Requirements

The proposed regulation aims to strengthen — and simplify — data protection provisions. Companies with more than 250 employees or those of any size with operations that involve so-called "risky processing" — processing operations that, because of their nature, scope or purposes, present risks to the privacy rights of individuals — must appoint a privacy officer. This requirement applies to both data controllers and data processors, and companies that fail to comply may attract significant fines of up to up to €1 million or 2 percent of their "global turnover."

The proposed regulation removes the requirement that companies notify their national data protection regulator that they are processing personal data and instead requires companies to undertake a "Data Protection Impact Assessment" examining their safeguards for protecting personal data where their processing is likely to be considered "risky." Where the impact assessment does indicate a high risk, the company should consult the national data protection regulator.

The proposed regulation also would require companies to implement compliance policies and practices reflective of current best practices, including recording the details of the processing of personal data, documenting retention periods and the reasons for the processing, and implementing and verifying the effectiveness of appropriate security measures and technologies to minimize collection of and access to personal data.

The regulation imposes a standardized security breach notification requirement on all data processors. In the case of a data security breach that leads to unauthorized access to, or the disclosure or destruction of, personal data, companies must notify their national regulator as soon as possible and where feasible, within 24 hours of the breach being discovered. Companies must also notify individuals whose privacy or personal data is likely to be adversely affected "without undue delay."

The imposition of these time frames for responding to data security breaches may pose significant challenges for companies that may not currently have policies or procedures in place to quickly identify adversely affected individuals and then provide the appropriate notifications to them — and to the authorities — within the required time.

Significant Fines

Under the proposed regulations, companies may be fined up to €1 million or 2 percent of their "global turnover" for serious offenses (such as processing sensitive data without an individual's consent). Less serious offenses (such as charging a fee when an individual requests his or her data) may be subject to fines of €250,000 or up to 0.5 percent of "global turnover."

The European Commission also proposed to strengthen the powers of national data protection authorities in member states to enable them to undertake investigations, make binding decisions and impose fines.

The EC will send the legislative proposals to the European Parliament and EU member states for discussion and approval, which may take as long as two years, during which time the proposed regulation may be amended. The regulation, as proposed, includes a two-year period of implementation after the new framework comes into effect. The approval and implementation process would give companies as much as four years of lead time to develop policies and processes to comply with the requirements of the regulation.

--By Ieuan Jolly, Loeb & Loeb LLP

Ieuan Jolly is a partner in Loeb & Loeb's New York office.

The opinions expressed are those of the author and do not necessarily reflect the views of the firm, its clients, or Portfolio Media, publisher of Law360. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

All Content © 2003-2012, Portfolio Media, Inc.