Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Changes To The EU Privacy Directive — Coming Soon

Law360, New York (December 8, 2010) -- The European Union has arguably the most comprehensive legal regime with regard to privacy and the transfer of personal data. The EU's 1995 Directive 96/46 /EC is the cornerstone for data protection in Europe. It establishes a regulatory framework in the EU for data "processing" — including the collection, storage, use, transfer or deletion of all personal data. Although there are various other EU directives dealing with privacy issues, it is often referred to in the U.S. as the "Privacy Directive."


Axel Spies

Since 1995, the provisions of the Privacy Directive have become the legal basis — with some variations and modifications — of the data-protection acts in all EU member states. They contain detailed rules on data collections and data transfers for all U.S. companies doing business in the EU. The national Data Protection Agencies in Europe enforce these provisions — sometimes vigorously. Therefore, the review of the Privacy Directive, as recently announced by the European Commission, has a major impact, affecting data collection, use of data, outsourcing, and privacy notices and policies.

The cross-border transfer of personal data (names, addresses, pictures, etc.) has become almost unavoidable in today's world of increasing economic globalization. The Privacy Directive requires that EU member states prohibit the transfer of personal data to non-EU countries whose laws do not provide similar protections to those embodied in the Privacy Directive, unless some other approved legal mechanism of assuring adequate protection of the data is in place.

Notably, the EU does not consider the U.S. to be a country that provides "adequate" data protection under its laws. This means that a U.S. company that needs or receives personal data from an EU member state must meet the requirements of the Privacy Directive on a company-by-company basis. The necessary safeguards include using so-called EU model clauses or in some cases declaring adherence to various data-protection principles with the U.S. Department of Commerce under the EU/U.S. Safe Harbor Principles.

Whatever method a U.S. company chooses, it should monitor the revision of the EU Privacy Directive through its compliance officers, in-house legal departments or outside advisers. The review may require changes to how databases are set up, new contracts with vendors and new privacy policies, and it could change the way data from Europe is used.

Those who want to get involved in the drafting process should step forward as early as possible. An EU strategy document issued by the European Commission on Nov. 4 contains various outlines for amendments to the Privacy Directive — the result of a public consultation that initially began in 2009. The ambitious across-the-bench revision is being spearheaded by the European Commission's Directorate-General for Justice, which is also the primary contact on the EU level for comments.

The European Commission claims it will have finalized a proposal for the necessary amendments in 2011, which will then head off to the European Parliament and the Council of Ministers for deliberation and final adoption. For this purpose, the

document released on Nov. 4 (COM (2010) 609 - Final) is practically a roadmap with a number of goals — some of them are quite a tall order:

1) A general principle of transparent data processing of personal data

The European Commission states in this document that since 1995 "rapid technological developments and globalization have profoundly changed the world around us, and brought new challenges for the protection of personal data ... The ways of collecting personal data have become increasingly elaborate and less easily detectable." Therefore, the European Commission urges companies to do more to ensure transparency of their data processing for all individuals, stating that "the information must be easily accessible and easy to understand, and that clear and plain language is used."

The European Commission considers specific obligations to protect children, drafting EU standard "privacy information notices" that companies could use to inform their data controllers and creating uniform rules to inform individuals in case of a data security breach — a goal that has not yet been achieved in the US. Even more ambitious is the goal of implementing the data-protection measures directly into devices through Privacy Enhancing Technologies (PETs) and Privacy by Design.

2) A "right to be forgotten" online

Pursuant to the existing rules of the Privacy Directive, individuals should always be able to access, rectify, delete or block their data, unless there are legitimate reasons, provided by law, for preventing this. However, the new EU proposal goes beyond this: the EU seeks to create legislation that will minimize the collection of personal data and at the same time enhance transparency to individuals about how, why and by whom their data is collected, and for how long it is kept.

One of the European Commission's suggestions is a "right to be forgotten" online. This new requirement may imply that individuals have "their data no longer processed and deleted when [it is] no longer needed for legitimate purposes. This is the case, e.g., when processing is based on the person's consent and when he or she withdraws consent or when the storage period has expired. What this goal means, e.g., for social networking sites, and how a total removal of personal data can be ensured, remains to be seen. Clarification will also be needed on who will be in charge of enforcing this right to be forgotten on the Internet, especially in social networks, and the sanctions companies will face in case the personal data is not entirely purged.

3) A more uniform application of the privacy rules throughout the EU

The European Commission hopes to enhance uniformity among EU member states' national laws and their interpretation. This has been a goal for many years. The European Commission acknowledges that on the level of the EU member states, the Privacy Directive has created significant administrative burdens for companies (e.g., prior notifications to the national data protection agencies) and, in some cases, conflicting rules. The European Commission aims to reduce these burdens and conflicts through new legislative measures.

This could include requiring larger companies to appoint an internal data-protection officer who would supervise the data-protection rules internally — which is already a requirement in EU member states such as Germany and Hungary. Another suggested method for providing a high level of data protection throughout the EU would be "creation of EU certification schemes (e.g., 'privacy seals') for 'privacy-compliant' processes, technologies, products and services." It is not clear who would develop these seals and supervise their use.

4) Revisiting the rules for data transfer outside of the European Union

The European Commission also intends to improve and streamline procedures for international data transfers, although it is not very specific on the details. Recently, data transfers outside of the EU — particularly with the U.S. — have been a bone of contention between the U.S. authorities and the European data-protection authorities and advocates. For instance, the U.S. government has been accused of being too lax in its efforts to enforce violations of the EU/U.S. Safe Harbor Principles against U.S. companies.

There is still a lot of noise on both sides of the Atlantic regarding the transfer of passenger data. The European Commission reiterates the need for actively promoting the EU privacy approach with non-EU countries that receive EU personal data — an effort that the U.S. government with its more industry-based "bottom-up" approach may challenge. According to the European Commission, the EU must "remain a driving force behind the development and promotion of international legal and technical standards for the protection of personal data, based on relevant EU and other European instruments on data protection."

5) Reconcile privacy with needs of law enforcement

The European Commission is not very specific on how to balance law enforcement's need for personal data with its goal of promoting individual privacy. It notes that the specific needs of this sector "will be" taken into account. In particular, the European Commission intends to enhance and broaden the EU Framework Decision 2008/977/JHA37 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters: "The Framework Decision is an important step forward in a field where common standards for data protection were very much needed. However, further work needs to be done."

In the past, the EU's authority to impose data-protection rules that affect law enforcement has been challenged at various occasions. The European Commission is confident that the EU's "Lisbon Treaty has … abolished the previous 'pillar structure' of the EU and introduced a new and comprehensive legal basis for the protection of personal data across [the EU]."

6) More efficient enforcement

The European Commission finally wants new rules to strengthen and harmonize the enforcement powers of national data-protection authorities. It states that the "Commission considers that Data Protection Authorities should strengthen their cooperation and better coordinate their activities, especially when confronted by issues which, by their nature, have a cross-border dimension. This is particularly the case where multinational enterprises are based in several Member States and are carrying out their activities in each of these countries."

Although many of the proposals are clearly a long shot and read like a laundry list for the next 10 or more years, U.S. companies with business in Europe or that receive EU data will be affected by all of these proposed changes. Given the timeline and complicated EU adoption process of the amendments, now is a good time to speak up — Jan. 15 is the deadline for submission with the European Commission — and influence the review process through submissions with the European Commission, through trade associations and/or political channels.

--By Axel Spies, Bingham McCutchen LLP

Dr. Axel Spies (a.spies@bingham.com) is a German lawyer and foreign legal consultant in Bingham McCutchen's Washington, D.C., office.