Final Negotiations Set To Begin On EU Data Privacy Law

Law360, New York (June 22, 2015, 10:28 AM ET) --
More than three years after the initial proposal for the EU Data Protection Regulation was published by the European Commission, it has been agreed by Europe's Council of Ministers. The negotiations will now start between the commission, the European Parliament and the Council, in what is known as the "Trilogue" process, to agree the final text of the regulation, which is widely expected to be adopted by the end of 2015 or early 2016. The regulation, once adopted, will have a significant impact not only on EU companies but also on U.S. and other international companies that conduct business in the EU.

William Long

The European Commission asserts that the regulation, which is intended to create a new single law on data privacy in the EU, will lead to savings of around €2.3 billion a year by reducing administrative burdens and costs. However, not everyone is convinced, and many believe the regulation will significantly increase compliance costs and privacy obligations for businesses. In addition, in the draft agreed by the council, there are a number of provisions allowing EU member states to determine their own national law requirements, leading to possible inconsistency and undermining one of the key objectives of the regulation: specifically, harmonization of privacy law across the EU.

Some of the key provisions in the regulation, as amended by the council, include:

- Territorial Scope: The council agrees with the commission and the parliament that the regulation should apply not only to businesses in the EU but also to businesses based outside the EU, such as those in the U.S., that offer goods or services to Europeans. Essentially, this means that U.S. and other international organizations collecting data on EU residents through, for example, websites will need to comply with the requirements of the regulation.
- Enforcement and Liability: Fines of up to 2 percent of annual worldwide turnover (gross revenue) have been proposed by the council for noncompliance with the regulation. With the parliament having proposed 5 percent, it is clear the fines on businesses for noncompliance will be significant whatever the outcome of the final negotiations.
- Accountability: The concept of accountability is crucial to the proposed regulation and requires businesses to adopt policies and procedures that demonstrate privacy compliance. Central to this concept is the requirement that businesses carry out privacy impact assessments, appoint a data protection officer, maintain detailed records of the personal data used by the business and implement technical and organizational privacy measures, such as encryption. While the council has tried to limit some of these new requirements, they could still lead to a significant increase in compliance costs for businesses.
- Data Breach Notification: One of the key issues with the proposed regulation has been the requirement to report security breaches. Under the council's proposal, a business is required to report a data breach to the relevant DPA within 72 hours. Importantly, the individual affected will also have to be informed of the breach, subject to a limited number

of exceptions. These mandatory data breach reporting requirements will likely add to the increasing focus among businesses on information security.

- Right to Erasure: Under the proposed regulation, individuals will have several new data protection rights, including a right to erasure of their personal data. There are concerns about how the right to erasure will be implemented in practice (as it is questionable whether it is technically possible to erase all personal data on the Internet) and how this new right will be balanced with competing regulatory obligations on businesses to retain certain data and documents and the right to free speech.
- Profiling: Another large concern for businesses in the age of big data is the regulation's restriction on profiling. This provides that an individual has a right not to be subject to a decision based solely on profiling, which significantly affects the individual unless, for example, with the explicit consent of the individual. Many think the restriction on profiling could undermine a wide range of valuable business practices across multiple sectors by preventing positive forms of analysis (for example, those that are used to prevent discrimination or to detect fraud). Companies will need to consider how the proposed restrictions on profiling will impact their business practices.
- International Transfers: The regulation will maintain the current restriction on transfers of personal data to countries outside of the EU that are not deemed to have adequate data privacy laws, such as the U.S., although the council proposes that specific industry sectors in countries outside the EU could be recognized as providing adequate safeguards. The council has also proposed that international transfers from the EU be permitted where necessary for the legitimate interests of the business, providing the transfer is not "large scale or frequent." Importantly, the council has not included the provision, required by the parliament, which makes requests for personal data made by non-EU authorities unenforceable.

The challenge during the final negotiations on the regulation, over the next few months, will be to try to reconcile the differences between the texts of each EU institution while ensuring that the objectives of the regulation are achieved and an appropriate balance is struck between encouraging the digital economy and protecting the interests of the individual. Although the details on some aspects of the regulation are still being negotiated, many believe that the regulation will, once adopted, have a considerable impact on businesses and industry. In readiness for the regulation, businesses should consider:

- Determining the applicability of the regulation to non-EU based businesses;
- Carrying out an internal gap analysis of current data protection policies and procedures of the business as compared with the new requirements and rights under the regulation, such as use of privacy impact assessments, keeping records of personal data used and the right of erasure; and
- Reviewing any profiling activities carried out by the business and assessing whether these are in compliance with the proposed restrictions under the Regulation.

—By William Long and Francesca Blythe, Sidley Austin LLP

William Long is a partner and Francesca Blythe is an associate in Sidley Austin's London office.

clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.