crowell moring

CLIENT ALERT

EU Data Protection Rules Might Transform the Internet

Oct.29.2013

With initial approval in the European Parliament civil liberties committee (the so-called LIBE Committee), the EU is moving ahead with overhauling its existing 15-year-old Data Protection Directive, replacing it with the General Data Protection Regulation (GDPR). The European Commission introduced the draft GDPR in January 2012 and seeks to harmonize regulations across the 28 member-states, replacing varying national laws with a single, consistent regulation on data handling and individual rights.

This new regime could fundamentally change the privacy and data transfer practices of every large company operating in Europe or offering goods or services to data subjects in Europe, the flows of data within financial services and other firms, and the business practices underlying internet products, cloud computing, or social networks offered to European consumers.

The LIBE Committee considered the draft last week after intensive lobbying, rewriting, and negotiations, where more than 4,000 amendments were offered. The revelations from former NSA contractor Edward Snowden intensified the sense of urgency regarding this legislation within the European Parliament. Language curtailing the transfer of personal data to non-European governments was included in the initial draft of the regulation, then struck after pressure by the United States, and finally reinstated in the LIBE's version of the draft once the Snowden material became public.

In many respects, the GDPR would change the relationship between the consumer and an online portal or Internet company.

- It would create a new "right to erasure," a slightly lesser standard than the "right to be forgotten." This allows consumers to request that all references and information about themselves be removed from a company's information systems and also any third-party systems.
- A new right to data portability would also be created. This would allow individuals to move their personal information between services and networks.
- The law would also require valid and explicit consent from consumers prior to collection of personal data, and parental consent for collection of data on children younger than 13.

Companies with operations or customers in Europe could have a host of new requirements under the proposed standards to ensure they do not violate new consumer rights.

- Large employers would have to create Data Protection Officers within their organizations, which is currently not yet the case in all Member States. The Officers would be responsible for all aspects of breach response as well as interacting with newly created EU regulatory offices.
- Privacy would have to be incorporated into web design, cloud computing, and other networked activities.
- Default settings for European consumers should minimize data collection and retention.
- Companies would have to conduct Data Protection Impact Assessments when data is compromised or an EU resident's rights are violated.

- Companies (including U.S.-based companies) would be forbidden from providing information about EU residents to foreign governments "without a legal basis."
- The proposed law would also establish civil penalties of up to five percent of worldwide revenue if a company is found in willful noncompliance of the regulations.

The LIBE Committee has also given a mandate to its rapporteur (EU Member of Parliament Mr. Albrecht) to start negotiations with the European Council, which also has to approve the text, and the Commission in a so-called trilogue.

Whereas it was first expected for these negotiations to start soon, the conclusions of the European Council meeting in Brussels last week (October 24 and 25) seem to indicate that the Council wants the adoption of the final text of the GDPR to be postponed to 2015 at the earliest, with implementation in 2017. These conclusions are, however, ambiguous, so that it is possible that the Commission and the Parliament will still try and obtain an agreement with the Council on the final text before the 2014 elections, even without the support of certain of the Member States within the EU Council (the UK and Sweden in particular).

This proposal is being considered as the United States and the EU negotiate a free trade agreement. There are signs that many of these rules could be discussed during these talks. Some in the European Parliament want to go further and also take a hard look at the Safe Harbor Framework. On October 7, a European Parliament Inquiry established to investigate the recent U.S. National Security Agency surveillance revelations indicated that its final report would recommend suspension of the Safe Harbor Framework.

Clearly, companies must maintain their vigilance regarding the trans-Atlantic divide on privacy, innovation, and the roles of government in the online marketplace and remain prepared and flexible so that they are ready to meet the requirements of the new legislation that is ultimately passed.

For more information, please contact the professional(s) listed below, or your regular Crowell & Moring contact.

Frederik Van Remoortel
Partner – Brussels
Phone: +32.2.282.1844
Email: fvanremoortel@crowell.com