ROPES & GRAY

ALERT

Privacy & Data Security

December 21, 2015

EU Reaches Agreement on Significant New Privacy Law

Following almost four years of debate, on December 15 the European Commission, the Parliament, and the Council agreed on the text of the General Data Protection Regulation (GDPR). This agreement was quickly followed by the approval of the text, on December 16, by the European Parliament's Civil Liberties, Justice and Home Affairs Committee.

The Regulation seeks to unify somewhat fragmented existing data protection rules in the European Union, increase certainty in their application, account for advances in technology and strengthen individuals' control over their personal data. However, the GDPR will still allow individual Member States some room to manoeuvre, but it will be some time before we see how this works in practice. The Commission expects that the final text will be formally adopted by the European Parliament and the Council of the European Union in early 2016; the GDPR will come into force two years after that without requiring any additional national implementing legislation from individual EU Member States.

Anyone already doing or intending to do business in the European Union or to offer services to individuals in the European Union should begin preparing for the new legislation. In particular, the GDPR introduces the following key changes to the existing European data protection regime:

- Fines have increased to up to EUR 20,000,000 or 4% of global annual turnover, whichever is greater – for global businesses, this could amount, in the case of serious breaches, to fines in the billions;
- Businesses outside the European Union offering goods or services (whether or not for a cost) and processing personal data of individual in the European Union, will be subject to the GDPR, including a requirement to formally appoint an EU representative in writing to act on their behalf;
- Businesses whose core activities include processing activities involving the systematic monitoring of EU individuals or the processing of sensitive personal data will be required to appoint a data protection officer having expert knowledge of data protection law and practices. Corporate groups will be entitled to appoint a single officer for this purpose;
- Those merely processing personal data on behalf of another person will for the first time be liable for breaches of the GDPR. Liability will include where they have breached provisions applicable to them (for example, to implement appropriate technical and organisational measures to ensure risk-appropriate security) or where they have acted outside the instructions of the data controller;
- The GDPR will create the so-called "one-stop shop", under which EU individuals and those processing personal data will benefit from only needing to coordinate with a single lead supervisory body according to their establishment – this could significantly reduce administrative burdens for businesses subject to the regime;
- Requirements to register with or notify national data protection authorities will be abolished. However, businesses subject to the regime will instead be required to maintain an internal written record of processing activities undertaken (which is likely to be similar to the information required to be submitted in those jurisdictions where registration is currently mandatory); and
- Businesses will generally not be entitled to charge for subject access requests – for many, this could represent a significant ongoing administrative burden and potentially cause substantial cost implications. However, the GDPR qualifies that in the case of manifestly unfounded or excessive requests (e.g. repetitive requests), businesses will be entitled to charge a reasonable fee.

Businesses will also be required to take the following steps, among many others:

- Delete an individual's data if the individual no longer wants his or her data to be processed or if it is no longer needed for the purpose for which it was collected and there are no legitimate or lawful grounds for retaining the data. This "right to be forgotten" will extend to requiring businesses who have published personal data publically online to take reasonable steps to inform others processing that data, to delete any links to or copies of that personal data;
- Provide information in a clear and understandable way regarding the ways in which individuals' data is processed; and
- Unless a personal data breach is unlikely to result in a risk for individuals' rights and freedoms, notify all personal data breaches to the relevant national supervisory authority as soon as possible and not later than 72 hours of becoming aware of the breach. The relevant individuals affected should also be informed where the breach poses a high risk to their rights and freedoms.

The Regulation also includes specific reforms intended to benefit small and medium enterprises, including the following:

- If data processing is not a small or medium enterprise's core business activity, the enterprise will not be required to appoint a data protection officer; and
- Small and medium enterprises will be required to carry out impact assessments only where the risk is high.

Officials also agreed on the Data Protection Directive, which regulates the protection and transfer of personal data in connection with law enforcement proceedings.

We will be providing further updates and more detailed guidance of the GDPR over the coming months, and in particular, once it has been formally approved in early 2016. Ropes & Gray will be hosting Data Privacy Day on January 28, 2016 in our Boston Office where a panel of privacy experts will participate in an in-depth review of the approved draft and a lively discussion on what this means for doing business in Europe. For more information on this event, please click here.