Dilworth Paxson

E-ALERT

Related Practices

Intellectual Property

Media Contact

Peter Dunn
Director of Client Relations and Communications
Philadelphia, PA
pdunn@dilworthlaw.com

NEW EUROPEAN UNION GENERAL DATA PROTECTION REGULATION COMING IN 2018

04/04/2017

Background

Data protection in the EU is currently governed by Data Protection Directive 95/46/EC (the "Directive"), which was implemented in 1995. Following the rapid change in technology since 1995, as well as the increased rate at which data is shared over the internet, the EU has revised its data protection laws to keep up with these changes. The new law, the EU General Data Protection Regulation (the "GDPR"), is designed to harmonize and modernize data protection across the EU. As an EU directive, the GDPR will be directly applicable in all member states, and will not require national implementing legislation.

The GDPR will enter into force on May 25, 2018.

Who does the EU GDPR affect?

Any company that either (i) offers goods or services to people within the EU, or (ii) monitors the behavior of people within the EU, will be subject to the GDPR.

Changes to data protection law

The GDPR's biggest change to EU data privacy law is that it increases the jurisdictional scope of data protection laws in the EU. Unlike the Directive, the GDPR will definitively apply to any company that processes the personal data of any person residing in the EU, regardless of where the processing company is located.

The GDPR also narrows the scope of what will be considered the valid consent of a data subject. Any request for consent must be intelligible, easily accessible, and must include the purpose for the data processing. Furthermore, it must be as easy for a data subject to withdraw consent as it is to give it.

Under the GDPR, data subjects who reside within the EU have the right to:

- Notification within 72 hours of a data breach that is likely to "result in a risk for the rights and freedoms of individuals".
- Confirmation from a data controller whether personal information is being processed, where, and for what purpose, as well as the right to a copy of such information in an electronic format.
- Compel the data controller to erase and stop dissemination of his or her personal data, subject to certain conditions. This is more commonly known as the "right to be forgotten".

Penalties

The GDPR has a tiered approach to fines:

- A company can be fined up to 2% of its annual global turnover or €10 million (whichever is greater) for not notifying the supervising authority or an individual data subject about a breach.
- Fines of up to 4% of annual global turnover or €20 million (whichever is greater) are possible for more serious infringements, including not having sufficient customer consent for processing data.

The percentage fines apply to an "undertaking", a broad term that under EU case-law has sometimes been held to include subsidiaries of a parent company.

Brexit

The UK Government has made indications that it will implement an equivalent or alternative legal mechanisms to the GDPR post-Brexit. It is generally expected that any new UK legislation on data protection will follow the GDPR, given the UK Government's support of the new EU Regulation.