Use Data from the EU? It's Time to Update Your Privacy Policies and Procedures

Insights
10.07.16

This is the first post in a three-part series.

May 25, 2018. If you are a company that comes into contact with European data, whether you are operating in Europe or elsewhere, and you have not taken note of this date yet, you should. That is when Europe's new data protection framework – the General Data Protection Regulation (GDPR) – will enter into force, replacing Data Protection Directive 95/46/EC (the "Directive"). Building on the premise that the protection of personal data is a fundamental right, the GDPR seeks to protect the personal data of individuals in the EU and ensure the free flow of personal data between Member States of the European Union (EU) and in Iceland, Liechtenstein and Norway, which are part of the European Economic Area (EEA).

Whereas the Directive required EU Member States to implement its key principles regarding the protection of personal data through national data protection laws, the GDPR applies directly to all Member States without the need for national legislation. The GDPR's harmonization of data privacy laws still embraces the key principles of the previous Directive, but it also introduces many significant changes. Here are just a few:

Geography Does Not Matter
Perhaps the most significant change from the previous Directive is the GDPR's global reach. Even if your company does not have operations in Europe, the GDPR still applies if your organization processes personal data of individuals in the EU and such processing is related to either (i) the offering of goods or services (no payment is required), or (ii) the monitoring of their behavior. The new rules were clearly intended to include internet activity, and it means that online platforms and other website operators that are accessible from Europe and have any sort of tracking mechanism (i.e., cookies) will be subject to the GDPR.

Accountability and Privacy By Design are Now Mandated
Privacy by design is an approach to designing projects, processes, products or systems that promote privacy and data protection from the start. This approach was not a requirement of the previous Directive but it has been embraced by the GDPR, which requires data controllers to hold and process only the data absolutely necessary for the completion of its duties (data minimization).

More Stringent Consent Requirements

More Stringent Consent Requirements

The conditions for processing data based on consent have been updated under the GDPR. First, written consent must be presented in a manner that is clearly distinguishable from other matters. For example, the terms and conditions of sale for an online purchase should be presented separately from the consent to share personal data with third parties for marketing purposes. Additionally, the consent must be intelligible and use clear, plain language (no legalese). Finally, it must be as easy to give consent as it is to withdraw it.

Steeper Penalties

The GDPR uses a tiered approach to fines, with fines of up to 4% of annual global revenues or €20 Million (whichever is greater) for the more serious violations (for example, not having sufficient consent to process data). Other infringements such as failing to notify the supervisory authority and data subjects of a breach can attract fines of up to 2% of annual global revenues or €10 Million. The significant increase in fines under the GDPR should get the attention of board level executives, making compliance a top priority for 2017.

Related People

Melissa A. Dials
Partner
440.740.2108
Email