

February 1, 2018

New EU Privacy Law Targets U.S. Businesses, Too

Corporate

Print

PDF

Stiff Penalties Will Likely Force Compliance With GDPR

A sweeping new law aimed at protecting the privacy of people living in the European Union will likely force virtually all businesses – small and large – here in the United States to overhaul the way they collect and use personal information received and stored digitally, or face potentially huge fines.

The European Union's [General Data Protection Regulation](#) (GDPR), which goes into effect on May 25, 2018, represents a paradigm shift in how companies across the world will be required to collect and use personal information. Its scope is not limited to companies in the EU; it covers any business that collects or processes the "personal data" of EU residents, irrespective of where in the world the company is located or if it is an online-only enterprise. Because of the inherently global nature of the internet, the GDPR's application will arguably extend to nearly every company in the world with a website and/or an app. Furthermore, the penalties for breaching the GDPR are potentially devastating: up to the greater of four percent of a breaching company's annual global revenue or 20 million euros.

Many privacy experts are already predicting that a majority of companies will not be in compliance with the GDPR by May. Gartner, Inc., a leading IT research firm, predicts that more than 50 percent of companies affected by the GDPR will not be compliant by the impending deadline, in part because the new regulation will require a complete overhaul of systems and policies for obtaining, using, protecting and deleting personal information. For most businesses, a quick or inexpensive fix to achieve compliance isn't possible.

A large number of U.S. businesses, primarily small-to-medium-sized companies, are likely not even aware that they will fall under the scope of the GDPR, and thus have little hope of being compliant by the impending deadline, Gartner predicts. Considering the stiff penalties for GDPR non-compliance, these companies run the risk of learning a very expensive lesson.

What is the GDPR?

The GDPR will become the primary EU law governing the protection of EU citizens' personal data, replacing the Data Protection Act of 1998 (DPA). The EU Parliament passed the measure in April 2016, intending to create a more consistent protection of EU citizens' data across the EU's 28 member states and to ensure that EU citizens have greater control over the collection, storage and use of their personal information.

Does the GDPR Apply to a U.S.-Based Business?

Given the broad scope of the GDPR, most U.S. businesses will be affected by its regulations. The new law will apply to any company that collects or holds data regarding EU citizens, even basic information such as a citizen's name or email address, if it is related to selling of goods or services to those individuals or to monitoring their digital activities. As a result, it arguably applies to nearly every company in the world that has any digital presence, such as a website or an app. The GDPR does not exempt smaller companies from compliance – not even for a solo proprietor.

Even if a U.S. company were to cease doing business with EU citizens to avoid having to comply with the GDPR, those efforts would likely prove fruitless. For example, if the U.S. business maintains a website that uses cookies and the site can be accessed by EU citizens, the company would still fall under the specter of the GDPR even if it's not making any sales to those customers.

Alternatively, despite having no EU clients of its own, if the U.S. business has clients or customers that serve or sell to EU citizens and the U.S. business will have access to these citizens' personal data, the client or customer will likely require the U.S. company to be GDPR-compliant as a condition of winning or maintaining its business. Without taking such precautions, the client or customer risks suffering the GDPR's draconian financial penalties merely for the U.S. company's failure to comply with the regulations.

Key GDPR Provisions

CONSENTS AND DISCLOSURES

The GDPR defines "personal data" extremely broadly to include any information related to a natural person that can be used to directly or indirectly identify the person, including the person's name, email address or computer IP address. For any business that processes or stores personal data of EU citizens, any online forms and interactions with these citizens will need to be adjusted to obtain explicit consent to the gathering of personal information.

Companies will need to adhere to the following rules when collecting such personal informatio