Get ahead of the game: The impact of the new EU data protection law

Here's what your company should be doing to prepare — even if you aren't doing business right now in Europe.

BY JAIME L. BARWIG AUGUST 2, 2016

If your business markets to customers in the European Union (EU) or provides services that track the **online activities** of Europeans (for example, their shopping habits or which videos they click on), beginning in 2018, you will face the challenge of complying with a complex set of laws and rules forming the EU General Data Protection Regulation (GDPR). This is the case even if you do not have an office or operations in the EU and marks a significant change from current law.

Like the EU Data Protection Directive 95/46/EC (the "Directive"), which forms the basis of current EU data protection law, the GDPR will regulate the security and privacy of EU residents' personal data. Given the significant technological changes and advances since the Directive was passed 20 years ago, the GDPR is intended to modernize data protection law in the EU and standardize it across the 28 EU member states.

First, we should mention the upsides to the GDPR. The GDPR will introduce greater harmonization across the EU and a single legal framework that applies across the EU member states without varying national laws, as is the case currently. In addition, it should become easier for large multi-national businesses to cover intra-company **data transfers**.

Here are the highlights of the some key changes that all companies should be thinking about and planning for.

Expanded territorial scope
First, as mentioned above, many non-EU businesses that are currently not required to comply with EU data protection law will be required to do so once the GDPR takes effect. This is because the GDPR drastically extends the application of European data protection law to data processing that occurs, not only in the EU, but also in the United States and other countries if a company collects, stores or processes personal data related to offering goods or services to EU residents or monitoring Europeans' behavior.

As a result, if your business markets to EU residents or provides services that monitor the activities of EU residents, your company likely will need to comply with the GDPR, even if you have no European operations and are not required to comply with current EU data protection law.

In addition, service providers located in the EU will be directly liable under the GDPR, whereas currently they need only be contractually responsible under their client agreements for how they treat clients' personal data. In today's highly connected marketplace, where more and more businesses are engaging with customers and partners across the globe, many companies will now fall within the scope of the GDPR's jurisdiction and will need to comply with the GDPR.

Increased regulatory enforcement and fines
Under the GDPR, enforcement of violations is expected to increase. In addition, the GDPR will replace the current framework of varying penalties across EU member states with more severe penalties, with maximum fines of €20 million or 4 percent of worldwide revenues, whichever is greater.

Data breach notification requirements
When in effect, the GDPR will require companies to notify regulators within 72 hours of learning about a personal data breach, regardless of whether the breach is likely to cause harm to affected individuals. The notification must describe the nature of the personal data breach, the categories and approximate number of data subjects implicated, the contact information of the organization's data protection officer, the likely consequences of the breach, and the measures the controller has taken or proposes to take to address and mitigate the breach.

Companies also will need to notify affected individuals when a breach is likely to result in a high risk to "the rights and freedoms of individuals" and must notify data subjects of the breach "without undue delay." Additionally, service providers are required to notify the data owner/controller of a data breach "without undue delay." The GDPR includes content requirements for notifications and sets forth limited exceptions to the notification rules.

Data protection officers
All organizations subject to the GDPR will have to implement comprehensive data protection compliance programs and maintain records documenting their data processing practices. Also, companies must appoint a data protection officer (DPO) where (1) they are a public authority or body; (2) their core activities require regular and systematic monitoring of individuals on a large scale; or (3) their core business activities include processing certain types of data on a large scale, including data relating to criminal convictions and offenses.

If your organization may be subject to the GDPR, now is the time to start reviewing your existing data privacy and security policies and procedures, including requirements your company expects from its service providers and partners.

The GDPR will stand as one of the most comprehensive and stringent legal frameworks regulating the collection and treatment of personal data. Once in effect, many companies not currently subject to EU data protection law will find themselves within the ambit of the GDPR and its complex and extensive requirements.

Meeting the obligations imposed by the GDPR requires thoughtful planning. Companies should take the time now to identify whether they will be subject to the GDPR, and, if they are, how they will need to expand and update their data policies, data breach response plans, business processes and contracts with customers, vendors and business partners.

About the Author

Jaime L. Barwig is an IP associate at Bass, Berry & Sims PLC (Nashville, Tenn.). Jaime counsels clients on matters affecting intellectual property ownership, development, commercialization and protection, as well as data protection and privacy matters. She can be reached at 615-742-7832 or jbarwig@bassberry.com.

Reprinted with permission from the July 19, 2016 edition of InsideCounsel © 2016 ALM Media Properties, LLC. All rights reserved. Further duplication without permission is prohibited, contact 877-257-3382 or reprints@alm.com.