What American Companies Need to Know about the EU's New General Data Protection Regulation (GDPR)

Insights
10.10.17

The General Data Protection Regulation (GDPR) is a new data privacy and security law in Europe that will go into force on May 25, 2018. Every organization that does business with EU customers, regardless of the home base of the organization, and regardless of the size of the organization, must come into compliance or risks significant financial penalties and legal exposure. The new law permits fines of the greater of €20 million or four percent of an organization's worldwide annual revenue for the previous fiscal year.

The primary purpose of the GDPR is to provide EU citizens with greater control over how their personal data is collected, protected and used. There must be a legitimate and lawful reason for collecting data and limited to the minimum necessary information for the purpose for which data are collected. Data must be deleted when that purpose has been achieved.

The definition of personal data under the GDPR is extremely broad and includes any information relating to an identified or identifiable natural person (e.g., addresses, telephone numbers, email addresses, bank information, credit card details, photos, posts on social media websites, medical information, and even an IP address). There is also a separate definition for "sensitive personal data" (e.g., racial or ethnic origins, political opinions, physical or mental health and criminal history) which is entitled to even greater protection.

Companies which are in compliance with the existing Data Protection Act (DPA) certainly have a head start as not everything has changed, but most companies will have to implement additional privacy protections and adopt comprehensive data protection strategies to comply with the more expansive provisions of the GDPR. The following are steps which companies should consider taking now to prepare for implementation of the GDPR.

- **Data Protection Officer (DPO)**. The GDPR requires that companies hire a DPO if they engage in regular, systematic collection or storage of sensitive customer data. Even if not required, it would be a good idea for most companies to have a DPO with sufficient expertise to guide compliance efforts.
- **Data Breach Notification Requirement**. The GDPR requires that companies report data breaches to authorities and affected customers within 72 hours of becoming aware of the breach.

Thus, companies should have an incident response team in place and be prepared with carefully crafted messaging.

- **Train Your Workforce**. The GDPR requires that companies raise awareness of and train their workforces on how to handle personal data under the new law.
- **Obtain Consent and Provide Information**. Organizations must obtain consent before any data are collected and provide customers (including website visitors) with detailed information on data that are collected and how the data will be used.
- **Institute Procedures for Deletion of Personal Data Upon Request**. Under existing law, organizations are required to delete personal data only when it causes substantial damage or distress. Under the new GDPR, an EU citizen may request that all data collected on them be permanently deleted if the information is no longer needed for the purpose for which is was originally collected or simply when consent to use the data is withdrawn.

With the enforcement date of the GDPR only seven months away, organizations should start assessing their policies and procedures so that they are not caught short when the law goes into effect. Organizations with any questions about the applicability of the GDPR to their activities or how to prepare should contact their regular Fisher Phillips attorney or any of the attorneys in our Data Security and Workplace Privacy Group.