Foster Garvey

GDPR: Is Your Website Compliant?

Legal Alert
May 1, 2018

Contact

Brooks Lindsay

Related Services

Privacy, Cybersecurity & Data Protection

New European Union Privacy and Data Security Law Effective May 25, 2018

Companies with websites that attract European visitors may be subject to a tough new European Union privacy law starting on May 25, 2018. The European Parliament adopted the EU's General Data Protection Regulation (GDPR) in April 2016 to replace the 20-year-old EU Data Protection Directive. The GDPR will take effect on May 25 across the EU and will be enforced, under the EU-US Privacy Shield Framework, by the United States government against American companies that target EU residents online.

The new law imposes strict requirements on companies that operate inside Europe and companies that operate outside Europe and target European residents online. These requirements include obligations to appoint a Data Protection Officer, to make data breach notifications within 72 hours, and to comply with the GDPR's "right to be forgotten" by deleting a European resident's personal data when requested to do so. The burdens imposed by the GDPR will likely compel American companies targeting European online visitors to include GDPR data protection addendums in agreements with European and multinational companies. Companies impacted by the new law should develop compliance strategies with the assistance of legal counsel.

While the GDPR aims to give EU citizens greater control over their personal data and harmonize data protection law across Europe, the GDPR's compliance requirements may have burdensome implications for companies attempting to attract or do business with EU residents online. The law is intended to apply to companies operating out of the EU and to "all non-EU companies without any establishment in the EU, provided that the processing of data is directed at EU residents." Companies with websites targeting some or all of the content to individuals residing in Europe likely will be subject to the GDPR's

requirements, outlined below.

When it takes effect on May 25, 2018, the GDPR will do the following:

- **Data Protection Officer**: The GDPR requires each covered company to appoint a Data Protection Officer (DPO), who must be proficient in data protection laws and IT management and who will be legally obligated to report data breaches to the company's appropriate national Supervisory Authority, as designated under the law.
- **Prompt Notice of Data Breaches**: The GDPR requires covered companies to report data breaches to their respective Supervisory Authorities within three days, with few exceptions. Notice generally must be provided "without undue delay and, where feasible, not later than 72 hours after having become aware of it." If delayed, a data controller must provide a "reasoned justification" for the delay.
- **Right To Be Forgotten**: The GDPR solidifies the "right to be forgotten" into EU law, giving EU citizens the right to ask companies to remove personal data that is either no longer relevant or out of date.
- **Data Controllers and Processors**: The GDPR requires covered companies to use Data Controllers (based inside of the company at issue) and Data Processors (third parties that process data on behalf of a Data Controller) that are compliant with the GDPR.
- **Notice to Customers**: The GDPR requires notices to customers regarding personal data retention time and contact information for their Data Protection Officer and Data Controller.
- **Significant Penalties for Non-Compliance**: The GDPR empowers national watchdogs (Supervisory Authorities) to issue warnings, data protection audits and fines for violations of the new law. The fines can be up to €20 million or 4 percent of annual revenue, whichever is higher.
- **Data Security**: The GDPR strengthens data security requirements for companies, including requirements regarding regular systems testing, improved resiliency of processing systems and capabilities to restore access to personal data, and "data protection by design" to mask personal data through mechanisms such as anonymization, pseudonymization and encryption.
- **Data Portability**: The GDPR enforces the right to data portability by requiring that Data Controllers allow and enable individuals to transfer personal data from one electronic system to another (e.g., to a competitor) without unreasonable obstruction.
- **Consent**: The GDPR prohibits companies from gathering personal data without explicit consent. Personal data can relate to private, professional or public life and include a name, photo, email, bank details, social-network posts, medical info or IP addresses. Those under 16 years of age must obtain parental consent, unless a country lowers the age limit to 13.
- **Profiling**: The GDPR allows targeted individuals to contest or challenge a company's automated, algorithmic decisions regarding the collection and use of their personal data,

such as “profiling” and “target marketing” which may involve categorizing individuals and serving them different ads or offerings based on personal characteristics.

- **Onward Transfers**: The GDPR will allow data transfers to third countries outside the EU (“onward transfers”) only if the third country’s data protections have been deemed “adequate.”
- **Exceptions**: The GDPR contains provisions and exceptions which likely will be the subject of ongoing scrutiny and interpretation as the implementation of the law unfolds. For example, certain exceptions may apply to data processed in an employment context or national security context. Such data may be subject to individual country regulations.

The GDPR’s Application to American Companies

To facilitate the implementation and application of the GDPR to American companies, the United States and the EU negotiated the Privacy Shield Framework to replace the 15-year-old Safe Harbor Principles. The new framework was designed by the U.S. Department of Commerce and the European Commission to provide companies with a mechanism to comply with data protection requirements when transferring personal data from the European Union to the United States. In short, American companies importing personal data from Europe will be required to comply with the GDPR’s robust obligations on how they process personal data and will be obligated to respond to complaints made by EU citizens.

The Department of Commerce will regularly review covered companies and their self-certifications that they have complied with the Privacy Shield Framework. The Federal Trade Commission (FTC) will enforce the law. Noncompliant companies will face sanctions and possible removal from a list of compliant companies.

Next Steps for Companies with Websites Targeting EU Residents

Companies operating websites targeting EU residents, regardless of whether they have offices or operations in the EU, will need to evaluate the scope of their potential GDPR compliance obligations by May 25, 2018 when the law goes into effect. For more information about the GDPR and how it may affect you, please contact Christopher Emch, Brooks Lindsay, or Philip Paine with Foster Pepper’s Privacy, Cybersecurity & Data Protection group.