CARLTON FIELDS

Beyond the European Union: How the GDPR Affects US Companies

February 20, 2018

Executive Summary The effective date of the European Union's General Data Protection Regulation (GDPR), Reg. (EU) 2016/679, is fast approaching and will affect many organizations across the globe, even those not located in the EU. According to the market research firm Forrester, 80 percent of the firms required to comply with the GDPR will not meet the May 25 deadline. Moreover, of that 80 percent, Forrester estimates that 50 percent have considered the cost and risks of non-compliance and decided it is in their best interest not to comply. The other 50 percent will attempt to comply, but are not expected to succeed. As the deadline nears, firms will have questions about the GDPR and need help with compliance. This alert is intended to inform U.S. companies about the unusually broad scope of the GDPR. **1. Brief History** The GDPR replaces the Data Protection Directive ("Directive"), 95/46/EC, an EU data protection law that was written in the mid-1990s when the internet was still relatively new. The GDPR was created to update the data protection regime in place under the Directive in response to the ways in which people and entities currently use information in business and personal contexts, as well as to address issues that resulted in inconsistent data protection compliance requirements between EU member states under the old regime. The GDPR, which has already been adopted, will not take effect until May 25, at which time it will repeal the Directive. Like its predecessor, the GDPR establishes rules relating to the protection of natural persons with regard to the processing and free movement of personal data. Unlike its predecessor, however, the GDPR raises the bar in terms of compliance. It requires greater openness and transparency, imposes tighter limits on the use of personal data, and gives individuals more powerful rights to enforce against organizations. Satisfying these requirements is expected to be a serious challenge for many organizations. Also unlike its predecessor, the GDPR is far-reaching in that it will impact almost every organization based in the EU, as well as every organization that does business in the EU, even if based abroad. The GDPR focuses on the processing of personal data of persons in the EU, not on where the information is being processed or controlled. Thus, it is imperative that companies with and without an EU presence, and their counsel, understand the GDPR and its impact. **2. To whom**

does the GDPR apply? The GDPR is not sector-specific. It applies to any organization—no matter where it resides—that intentionally offers goods or services to "data subjects" (i.e., persons or individuals) in the EU (whether or not in return for payment), or that monitors the behavior of individuals within the EU, even if they are not EU citizens, to the extent such behavior takes place in the EU. The question of what constitutes "offering" goods or services to individuals in the EU will be determined on a case-by-case basis. There are four main concepts to consider in determining whether an organization falls under the territorial scope of the GDPR: **First**, if the company has an "establishment" in the EU, the GDPR will apply. An "establishment" implies the "effective and real exercise of activity through stable arrangements," regardless of the legal form of the arrangement. So an EU establishment could take the form of a branch, subsidiary, or joint venture. The GDPR does not automatically apply simply by having an office in the EU. **Second**, if it is "apparent" that the company "envisages" sales to residents of the EU (including foreign nationals living in the EU), the GDPR will apply. The general consensus here is that the GDPR will apply if, on balance, it is clear that the company markets goods and services to the EU by accepting EU currencies, having a website translated in EU languages, collecting EU emails, and/or any other conduct exhibiting an intent to collect and process information on EU data subjects for marketing purposes. As a practical matter, it is generally understood that under this second scenario the GDPR is less likely to apply to a non-EU company with small incidental sales to EU customers. Conversely, if the non-EU company notices a high volume of EU customers and starts to deliberately profile the EU customers by sending them targeted emails, then the GDPR is more likely to apply. **Third**, if the company, wherever located, uses an advertising technology platform to monitor EU data subjects, the GDPR will apply. "Monitoring" may include tracking or profiling an EU resident on the internet. **Fourth**, the GDPR likely applies if the company has employees located in the EU. The GDPR has specific rules regarding employee monitoring and personal information processing, including obtaining an employee's consent to have personal data processed and transferred across borders to a non-EU location. To recap, the GDPR applies to:

1. Controllers and processors in the EU, regardless of where the processing takes place.
2. Controllers and processors outside the EU where activities include: (i) offering goods or services to data subjects in the EU; (ii) monitoring data subject's EU behavior; or (iii) monitoring and processing personal data of EU data subjects.
3. Controllers outside the EU but in a place where the member state law applies via international law.

3. To what does the GDPR apply? The GDPR applies to the processing of "personal data" wholly or partly by automated means, or which forms or is intended to form part of a filing system. The type of personal data protected under the GDPR is noticeably broader than personally identifiable information or personal health information commonly subject to protection under U.S. laws. To use online advertising businesses as an example, many types of "cookies" will become personal data under the GDPR, because those cookies constitute "online identifiers." "Personal data" under the GDPR means any information relating to a data subject or reference to an identifier such as: a name;

an identification number; location data; an online identifier; or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that person. The GDPR also designates certain categories of personal data as "particularly sensitive," requiring stronger justification for processing. Sensitive categories include personal data that discloses racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, health, sex life and sexual orientation, genetic data, and biometric data. The GDPR does not apply to the processing of personal data:

1. in the course of an activity which falls outside the scope of EU law (*eg.*, activities of a member state in relation to national criminal law);
2. by the member states when carrying out activities which fall within the scope of Title V, Ch. 2 "Policies on Border Checks, Asylum, and Immigration;"
3. by people performing household activities provided there is no connection to a professional or commercial activity;
4. concerning threats to public security; or
5. of deceased persons or of legal entities (although, member states may provide for rules regarding the processing of data of deceased persons).

So for example, the GDPR would apply to protect the personal data processed by a company with a presence in the EU that provides travel services to customers based in an EU state. But the GDPR would not apply to protect the data of an individual who uses his or her own private address book to invite friends via email on a trip he or she is organizing. **4. What are the consequences of non-compliance**? The EU regulator in charge of enforcement, comprised of the National Data Protection Authorities (DPAs), will begin enforcing the GDPR on May 25. Companies subject to the GDPR have until that date to ensure their data processing activities comply with the requirements of the GDPR. The consequences of non-compliance can be severe. The GDPR authorizes DPAs to levy fines up to the maximum of 20 million euros or four percent of global annual turnover, whichever is higher. These numbers were specifically designed to attract C-suite attention. The GDPR also empowers individuals in the EU to seek judicial relief for damages and file administrative complaints with supervisory authorities. **Have Questions**? If you have questions about whether the GDPR applies to your business, please contact the Carlton Fields attorney with whom you usually work, or the authors of this alert.

Related Practices

Cybersecurity and Privacy
International
Technology

Related Industries

Technology