PUBLICATION

GDPR Goes into Effect Next Year; Is Your Privacy Program Ready?

October 18, 2017

You and your company may be located in the United States, but if any of your employees or customers are citizens of European Union (EU) member states, the EU will soon have a say in the collection, processing, storage, transfer, and protection of their personal information.

The General Data Protection Regulation (GDPR) was enacted by the EU Parliament and Council in April 2016 and will become effective May 25, 2018.

Unlike the United States, where a patchwork of privacy laws regulate different industries, the GDPR will be a comprehensive privacy law that governs any entity that collects or processes the personal data of any citizen of the 28 EU member states.

Critically for U.S. firms, the GDPR embraces an "extra territorial" approach, creating jurisdiction based on digital presence in the EU without reference to physical activity. Thus, the EU will enforce the GDPR's requirements on any entity that

- offers goods or services to the EU, or
- monitors behavior of EU citizens,

irrespective of that entity's lack of physical presence in the EU. For purposes of the GDPR, not having a "brick-and-mortar" presence in Europe will no longer be a defense for entities that interact with EU citizens and collect or process their data. Sanctions for violations can be steep, with EU regulators permitted to impose a financial penalty of ***up to four percent of a company's global revenue***.

Accordingly, it is vital that U.S.-based companies make a determination now as to whether their business activities will subject them to the GDPR's requirements and to begin making appropriate preparations.

Offering Goods and Services

Given the global reach of the Internet – where anyone in the world can access your business's products without being marketed to directly – determining whether you are "offering" your goods and services to the EU will be a critical undertaking.

Fortunately, the GDPR acknowledges that simply because a website can be accessed by EU residents does not mean that the site's host "envisaged" a business relationship with the EU. But at what point the scales tip will be fact specific; regulators will look at issues such as whether a site is available in a non-native language, accepts Euro or other EU member state currencies, or otherwise appears to target residents of the EU explicitly. If so, the proprietor will need to be compliant with GDPR or start taking steps now to unwind its EU offerings.

Nevertheless, even businesses that do not target EU customers still might find themselves in the GDPR's ambit if they are monitoring the Internet activities of EU residents.

Monitoring Behavior

The use of browser cookies is ubiquitous in modern e-commerce. While session cookies probably won't run afoul of any regulations, the use of persistent cookies to track an EU user's activities on the Internet arguably will be regulated by the GDPR. Moreover, as EU member states are beginning to view IP addresses as personally identifiable information in a way that U.S. courts and regulators have not, logging the IP addresses of EU residents also may constitute monitoring activity.

Suffice to say, there are a number of regular business activities that can pull an American company into the orbit of the GDPR, and with just over seven months until it becomes effective, now is the time to begin either winding down potentially offending actions or planning for compliance.

A High-Level Look at GDPR Compliance

Substantively, the GDPR places a number of compliance obligations on covered entities, with the following among the most critical:

- *Privacy Impact Assessment (PIA)*: A PIA will be a mandatory prerequisite before processing personal data. This documentation will need to be robust, especially if operations are likely to present higher privacy risks to individuals.
- *Expanded Personal Data*: "Personal data" under the GDPR is more than what U.S. regulators typically define as "personally identifiable information." Under the GDPR, personal data will also include information such as IP addresses, mobile device identifiers, biometric data, and geolocation tags.
- *Mandatory Data Protection Officer (DPO)*: Any entity that engages in "regular and systematic monitoring of data subjects on a large scale" or conducts large-scale processing of "special categories of personal data" (e.g., racial/ethnic origin, religious affiliation, or political opinions) must have a DPO with "expert knowledge of data protection law and practices." While the DPO may have other responsibilities (and in smaller organizations, could be an outside counsel or consultant), the DPO must have a direct line of reporting to the "highest management level."
- *Cybersecurity*: Entities must "implement appropriate technical and organizational measures" for cybersecurity, taking into account "the state of the art and the costs of implementation" and "the nature, scope, context, and purposes of the processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons." Examples of such measures include pseudonymization, encryption, sufficient and secured backups, and an auditable and testable system to ensure the effectiveness of security protocols.
- *Breach Notification*: "[A] breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data" requires notice to an EU supervisory authority "not later than 72 hours after having become aware of" the breach. Unlike most U.S. state data privacy laws, the GDPR requires notice irrespective of whether financial harm or fraud might result from the breach.
- *Opt-in Consent*: Before a subject's personal data can be processed, that individual must express consent that is "freely given, specific, informed and unambiguous." Such consent must consist of "a statement or a clear affirmative action," and "[s]ilence, pre-ticked boxes or inactivity" is not sufficient. Even more explicit personal consent is necessary for certain categories of sensitive data, and parental consent is necessary before processing a minor's personal data.
- *Information Governance*: Companies will have increased responsibility for knowing what information they control and how they must safeguard it. Individuals will have the "right to be forgotten," which can present a complex set of issues for companies. They will also have the right to have better control over their personal data and to be informed in clear and plain language regarding a company's privacy policies.

With GDPR enforcement becoming a reality in a matter of months, now is the time to assess whether it will affect your business activities. If you aren't sure whether you hold data on European Union residents, the place to start is by updating your data map. Members of Baker Donelson's Data Protection, Privacy, and Cybersecurity Team are ready to assist you in this process and help you decide what comes next.