GDPR: Ready for the EU's New Data Privacy Law?

What You Need to Know

What is the GDPR?

The European General Data Protection Regulation (GDPR) is a new law going into effect on **May 25, 2018** that grants European residents broad, never-before-recognized data privacy rights, and imposes significant demands on the companies that process or control European residents' personal data.

The consequence for violating the GDPR could be financially devastating—the fine for non-compliance is up to 20 million Euros or 4 percent of a company's worldwide annual revenue, whichever is higher. The GDPR has a broad reach, even impacting companies with no physical presence in Europe. Extensive preparation may be necessary for the companies pulled unwittingly into the GDPR through its extra-territorial reach. However, even companies previously working in the EU may be surprised at the demands of the new regulations. Compliance efforts should be made prior to May 25, 2018 for all affected companies.

How Did the GDPR Come About?

Originally proposed in January 2012, the GDPR was designed to harmonize data privacy laws across Europe to facilitate the free-flow of information across internal borders and to expand residents' rights concerning their personal data. After four years of debate and thousands of proposed amendments, the GDPR was approved by the EU Parliament in April 2016. It will go into effect in all member states in May 2018, replacing an outdated data protection directive from 1995 when only about 1% of the European population was using the internet.

The GDPR will also go into effect in the UK in May 2018 because the UK will still be a member state at that time. Further, the UK has released its own draft Data Protection Bill, which aims to incorporate the GDPR to deal with the inconsistencies created by UK's exit from the EU, and to provide continuity through the Brexit process. The UK aims to implement this Bill in May 2018 and it will have to be read alongside the GDPR until Brexit is completed.

How Do I Know if My Company Will Need to Comply With the GDPR?

The extra-territorial nature of the GDPR is one of its most impactful aspects because the regulation applies to all companies that collect or use the personal data of EU residents, regardless of those companies' locations or where the collection or use takes place. This means that companies with no European physical presence could be fined based on having a single European customer, or for advertising targeted at Europeans, or even for a website that is visited by Europeans. Moreover, non-European parent companies may be subject to GDPR fines due to actions of their subsidiaries. The fines are based on the worldwide annual revenue of an "undertaking" which can include the parent company as well as all other companies controlled by the parent. This

means that if, for example, a subsidiary company of an American parent company violates the GDPR, the American parent company could face fines calculated on a percentage of the worldwide annual revenue of all companies over which the parent exercises control.

In addition to the territorial aspect, the GDPR applies broadly to entities that are considered to be data processors and/or data controllers. Data processing is defined to encompass essentially any conceivable operation related to data that could be performed, including data collection. A data controller is any entity that controls the collection of data and how and why the data is processed.

What Type of Data Is Protected by the GDPR?

The GDPR regulates the collection and use of "Personal Data" which is defined more broadly under the GDPR than it is in other countries such as the United States. It includes virtually any information that may be linked to an individual such as a name, identification number, location data, an online identifier or data specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person. Thus, many common online identifiers such as email, IP and MAC addresses are subject to the requirements of the GDPR. In contrast, U.S. data privacy laws provide protection for Personally Identifiable Information (PII), which is defined somewhat more narrowly. Generally, PII must directly identify an individual. For example, a social security number would be considered PII, whereas IP addresses have been found not to be. The GDPR also protects a broader range of "Sensitive Data." Notably, the EU has a broader definition for health-related "Sensitive Data" which includes data collected by fitness wearables.

What Is Required to Comply with the GDPR?

The GDPR requirements for data processors and data controllers revolve around the privacy rights of EU residents – many of which are new. The GDPR also places the burden on companies to be responsible for and able to demonstrate compliance with the regulations.

The GDPR requires that Personal Data must be:

- Processed lawfully, fairly and in a transparent manner;
- Collected for specified, legitimate, and explicit purposes and not processed in a way which is incompatible with them ("purpose limitation");
- Adequate, relevant and limited to what is necessary in relation to purposes for which it is processed ("data minimization");
- Accurate and kept up to date (where necessary) ("accuracy");
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which it is processed ("storage limitation");
- Processed to ensure appropriate security of data ("integrity and confidentiality"); and
- Controlled by a controller that is responsible for the data and able to demonstrate compliance ("accountability").

The GDPR provides a set of rights to EU residents. Companies must provide each of the following to EU residents (some upon request, others whether requested or not):

- Right to access a copy of their data and information about how their data is being processed;
- Right to have inaccuracies rectified without undue delay;
- Right to erasure of personal data (Right to be "forgotten");
- Right to restrict data processing;
- Right to data portability (right to receive all of their personal data in a common format);
- Right to object; and
- Right to Breach Notification.

The requirement for "lawful" collection and use of Personal Data under the first GDPR requirement above may be among the biggest challenges for GDPR compliance because it requires a company to properly provide notice and obtain consent when collecting Personal Data. Before the GDPR takes effect, companies can rely on "opt-out" consent for the use of cookies or other data collection. However, the GDPR will require that individuals must actively "opt-in" to any collection of their Personal Data and forbids collectors from relying on pre-checked boxes. Requests for consent must be clearly distinguishable and presented in an intelligible and easily accessible form using clear and plain language. Consent must be as easy to withdraw as it is to give, and the person providing his or her Personal Data must be told upfront that withdrawal is possible. Moreover, companies collecting and using Personal Data cannot condition contracts and services on an EU resident granting GDPR consent if collection or use of the Personal Data is not necessary for the performance of the contract or service.

Additionally, when collecting information, companies must provide EU residents with extensive amounts of information to meet the transparency requirement. Companies that use or process Personal Data must provide, among other things, the identity and contact details of the data controller (i.e., the company that "owns" the data), the purposes and legal basis of collecting and using the data, details on other recipients and cross-border transfers, and period for which the data will be stored. EU residents must also be notified of the existence of any automated decision-making, such as profiling, to which they have the right not to be subject.

Companies are subject to additional requirements which include implementing appropriate technical and organizational measures to ensure and demonstrate compliance with GDPR policies. These measures may differ depending on the type of processing and can include "pseudonymisation" of data (a way of depersonalizing data) and implementing policies of data protection by default (e.g., automatic deletion of Personal Data once it is no longer needed). Additionally, companies may need to have privacy impact assessments (PIA) before using Personal Data in a manner that is likely to result in high risks to privacy rights and freedoms such as automated processing (especially profiling) and large-scale processing of special categories of data. Certain companies will be required to appoint Data Protection Officers (DPOs) to oversee data protection strategy and implementation to ensure GDPR compliance. Companies must

appoint a DPO if their core activities involve regular and systematic monitoring of EU residents on a large-scale basis or involve large-scale processing of "sensitive data."

How Do I Deal with a Data Breach Under the GDPR?

Under the GDPR, Breach Notification will become mandatory in all member states where a data breach is likely to "result in a risk for the rights and freedoms of individuals." Companies must report breaches to national Data Protection Authorities (DPA) within 72 hours of first having become aware of the breach where feasible. Companies must provide specific information, which can be provided in phases if it is not possible to provide it all at once. Additionally, companies must document breaches, including the effects of the breaches and any remedial measures taken. Data processors (i.e., vendors of the companies that collect the data) will also be required to notify the relevant company "without undue delay" after first becoming aware of a data breach.

Companies must additionally notify residents without undue delay if residents' privacy rights and freedoms are put at high risk. The GDPR includes exceptions to the notification requirement where preventative measures were taken to protect data (such as encryption), notification would require disproportionate efforts, or where the breach is unlikely to result in a high risk to the rights and freedoms of residents. If a company has not already notified residents, the supervisory authority may determine whether notification is necessary after considering the likelihood of rights and freedoms being put at high risk and whether any exceptions are met.

Conclusion

If your company collects Personal Data and has a presence in Europe, or has advertising targeted at EU residents, it has until May 25, 2018 to ensure its data privacy and security practices are in compliance with the GDPR. Knobbe Martens has GDPR capabilities to assist with these efforts.

About Us

Knobbe Martens Data Privacy and Security team is dedicated to helping clients achieve and maintain compliance with federal, state, and international data protection and security laws. Our inter-disciplinary team of attorneys is equipped to provide Data Privacy and Security legal services in the software, mobile apps and information technology, e-commerce, healthcare information technology, financial services, media & entertainment, and communications technology industries, among others.

The firm is composed of over 275 lawyers and scientists, dedicating its practice to all aspects of intellectual property and technology law, with more than 45 possessing computer science, engineering, and healthcare and regulatory backgrounds. The firm is headquartered in Orange County, California, with offices in Los Angeles, New York, San Diego, San Francisco, Seattle, Silicon Valley and Washington, D.C., and enjoys an international reputation for excellence. More information about the firm can be found at www.knobbe.com.