What U.S. Businesses Need to Know About the GDPR: Part I

03.28.2018

Your customers, business partners, and maybe even your own employees may be asking you whether you are ready for the "GDPR." You may also be receiving contracts from your business partners that contain new, unfamiliar language referencing the GDPR.

The General Data Protection Regulation ("GDPR"), the new set of rules governing data privacy in the European Union, goes into effect on May 25, 2018. The GDPR is drafted to have a wider reach than previous European data privacy laws and could require U.S.-based businesses with no employees or offices in the European Union ("EU") to comply or else face stiff penalties.

Before concluding that the GDPR is not relevant to your business – or before entering into what can be a costly and time-consuming process to update business practices with respect to handling of personal data – you should first determine whether your company is even subject to the GDPR. It is important to carefully assess the applicability of the GDPR to your business practices.

Part One of this article series addresses the scope of the GDPR.

Whose Data Does the GDPR Govern?

Individuals who are physically located within the boundaries of the EU are referred to as "data subjects" under the GDPR. The purpose of the GDPR is to protect the rights of data subjects.

ATTORNEYS

Roberta L. Christensen

Maureen E. Fulton

PRACTICE AREAS

Data Privacy and Security

Intellectual Property

What U.S. Businesses Need to Know About the GDPR: Part I

Some media reports about the GDPR have been misleading in stating that the GDPR applies to the personal data of "EU citizens." GDPR is meant to protect individuals physically located in EU countries; citizenship does not matter. The data of EU citizens working in the United States, for example, is not protected by the GDPR.

What Type of Data Does the GDPR Govern?

The GDPR is designed to protect "personal data," which is defined as "any information relating to an identified or identifiable natural person." That definition is intentionally broad: in addition to contact information, also included are credit card details, financial information, medical information, posts on social media websites, location information, and IP addresses.

Do Your Business Activities Implicate the GDPR?

If your business either *controls* or *processes* the personal data of data subjects (1) in relation to the offering of goods or services, or (2) in order to monitor their behavior, the GDPR applies. A controller determines the purposes for which personal data is processed. For example, a bank which stores its customers' data on a cloud-based software service is a controller. A processor is any business that processes personal data on behalf of a controller. For example, the provider of the software service above, which processes customer data on behalf of the bank, is a processor.

Even if no financial transaction takes place, the GDPR could still apply to your business' online activities. Simply maintaining a commerce-related website that can be accessed from the EU does not appear to implicate the GDPR; the website would need to show intent to attract EU customers, by offering the site in another language or mentioning consumers based in the EU, for example. But if your website uses cookies to track user data and your web traffic indicates you have EU visitors, you should assess whether you should affirmatively ask website visitors for consent to use their data so that you are complying with GDPR standards. If your business tracks data subjects online to analyze their personal preferences when surfing the Web, the GDPR could apply.

Part Two of this series will more closely examine GDPR processor and controller agreements.

Koley Jessen will continue to monitor developments related to GDPR guidance and advise as updates become available. If you have questions on whether your business needs to comply with the GDPR, and what steps you must take to comply with the GDPR, please contact one of the specialists in Koley Jessen's Data Privacy and Security Practice Group.