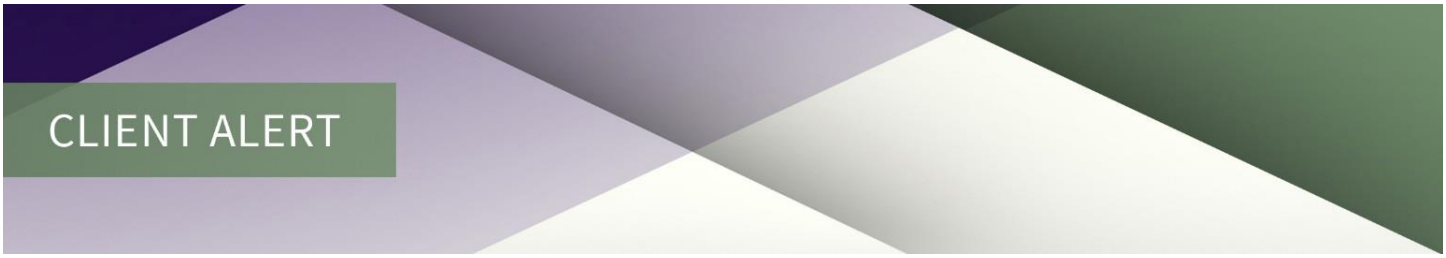

GDPR Is Coming: Are You Ready?

April 30, 2018

AUTHORS

Daniel K. Alvarez | Henrietta de Salis | Christian Rolf

Privacy and data security regulation in the European Union ("EU") is in the midst of a profound and significant change, with major implications for organizations both inside and outside of the EU. The General Data Protection Regulation ("GDPR"), adopted by the European Commission in May 2016, comes into effect on May 25, 2018. As we have explored in previous client alerts — here, here, and here — GDPR imposes a number of new requirements and obligations on both "data controllers" and "data processors." In addition, GDPR reaches beyond the borders of the EU; companies that process data in the United States, Canada, and other parts of the world may find themselves under the auspices of GDPR if the data they process is related to or collected from individuals in the EU.

With less than a month to go before GDPR comes into effect, now is the time to make sure you understand exactly how this regulation may affect your business. This memo is designed to raise awareness of some of the major jurisdictional and operational issues you should consider before May 25th to ensure that you are fully informed and ready to deal with a post-GDPR world.

Does GDPR Apply To You?

One of the most important aspects of GDPR for U.S. organizations is that its scope is extraterritorial. That is, it applies even if you do not have a physical presence in the EU. Specifically, for U.S. organizations GDPR applies in three circumstances:

1. If an entity holds an "establishment" in the EU and the data processing relates to such establishment (regardless of whether or not it takes place in the EU);

2. When an entity does not have an establishment in the EU, if it controls or processes personal data of EU persons in relation to "the offering of goods or services, irrespective of whether a payment of the data subject is required," to data subjects in the EU; and
3. When an entity does not have an establishment in the EU, if the controller or processor activities are related to the monitoring of data subject behavior insofar as that behavior takes place in the EU.

Each of these circumstances is potentially broader than appears at first glance. For example, GDPR says that "establishment" is less about specific legal constructs and more about "stable arrangements" that evince a pattern of doing business in the EU. Likewise, using cookies or other "tracking" technologies on your website may trigger GDPR obligations even if you are not specifically trying to sell your goods or services in the EU market.

Are Your Privacy Notices Sufficient?

One of the central pillars of GDPR is transparency; i.e., giving data subjects enough information to make informed decisions about the use of their personal data. GDPR includes a number of specific requirements for privacy notices, including information about the following:

1. The purposes and lawful basis for the processing;
2. Any third-party recipients of the data; and
3. The data subjects' rights to access, rectification and erasure.

Ensuring that your privacy notice is sufficient should be one of the primary tasks you undertake to improve your compliance posture.

Do You Have Consent Where You Need It?

GDPR requires companies that process personal data to identify a lawful basis for the processing prior to engaging in the processing. For many processing activities, lawful bases like performance of the contract or "legitimate interests" may be sufficient to justify the processing. But there will also be circumstances — particularly when you are handling "sensitive" personal data — where you may need the consent of the data subject to proceed with the processing.

In those circumstances, you will need to make sure the consent you obtain from the data subject meets the baseline requirements of GDPR: Consent must be "freely given, specific, informed, and unambiguous." And to the extent you received consent prior to the effective date of GDPR, you may need to look at whether that consent is sufficient under GDPR; if not, you may need to go back to the data subject and get GDPR-specific consent.

Are You Prepared To Handle Data Subject Requests?

One of the biggest operational challenges for many companies subject to GDPR will be responding to data subject requests. Under GDPR, data subjects have the right to access, to rectify and to erase, among other actions, data held about them by organizations. These rights are not absolute; for example, the right to erasure (also known as the "right to be forgotten") may be limited in cases where the company needs the data to perform a service or to comply with legal obligations. But companies must know what data they have about data subjects and where that data is located — everything from customer databases to email contacts — and have processes in place to record and respond to such requests.

How Are You Transferring Data From The EU To The United States?

GDPR carries forward from the 1995 EU Privacy Directive the requirement that cross-border data transfers are permissible only to the extent that the non-EU country to which the data is being transferred has "adequate" protections for the data subjects. The United States is not considered to have "adequate" protections, so transferring data from the EU to the United States is particularly complicated. Companies have multiple options for doing it — e.g., the EU-U.S. Privacy Shield Framework (which we've previously summarized for you here and here), binding corporate rules, and standard contractual clauses — but each presents different legal risks and operational considerations, and the right solution for one set of circumstances may not be the right solution for another. Companies that find themselves newly subject to EU privacy law because of GDPR's extraterritorial reach — or that are using GDPR to review and revise existing privacy controls — need to consider how they can ensure compliance with these particular requirements.

Conclusion

GDPR comes into effect in less than a month. It's not too late to start your compliance effort, but time is running short. Willkie has a team of attorneys from across our offices and practice groups ready to answer any questions you may have, and to help you navigate the complex maze of requirements and obligations that GDPR imposes.

If you have any questions regarding this client alert, please contact the following attorneys or the attorney with whom you regularly work.

Daniel K. Alvarez
202 303 1125
dalvarez@willkie.com

Henrietta de Salis
44 203 580 4710
hdesalis@willkie.com

Christian Rolf
49 69 79302 151
crolf@willkie.com