gould+ratner

New EU Privacy Law Targets U.S. Businesses, Too

Stiff Penalties Will Likely Force Compliance With GDPR

Peter C. Spier
Partner

pspier@gouldratner.com
(312) 899-1615

A sweeping new law aimed at protecting the privacy of people living in the European Union will likely force virtually all businesses – small and large – here in the United States to overhaul the way they collect and use personal information received and stored digitally, or face potentially huge fines.

The European Union's General Data Protection Regulation (GDPR), which goes into effect on May 25, 2018, represents a paradigm shift in how companies across the world will be required to collect and use personal information. Its scope is not limited to companies in the EU; it covers any business that collects or processes the "personal data" of EU residents, irrespective of where in the world the company is located or if it is an online-only enterprise. Because of the inherently global nature of the internet, the GDPR's application will arguably extend to nearly every company in the world with a website and/or an app. Furthermore, the penalties for breaching the GDPR are potentially devastating: up to the greater of four percent of a breaching company's annual global revenue or 20 million euros.

Many privacy experts are already predicting that a majority of companies will not be in compliance with the GDPR by May. Gartner, Inc., a leading IT research firm, predicts that more than 50 percent of companies affected by the GDPR will not be compliant by the impending deadline, in part because the new regulation will require a complete overhaul of systems and policies for obtaining, using, protecting and deleting personal information. For most businesses, a quick or inexpensive fix to achieve compliance isn't possible.

A large number of U.S. businesses, primarily small-to-medium-sized companies, are likely not even aware that they will fall under the scope of the GDPR, and thus have little hope of being compliant by the impending deadline, Gartner predicts. Considering the stiff penalties for GDPR non-compliance, these companies run the risk of learning a very expensive lesson.

What is the GDPR?

The GDPR will become the primary EU law governing the protection of EU citizens' personal data, replacing the Data Protection Act of 1998 (DPA). The EU Parliament passed the measure in April 2016, intending to create a more consistent protection of EU citizens' data across the EU's 28 member states and to ensure that EU citizens have greater control over the collection, storage and use of their personal information.

Does the GDPR Apply to a U.S.-Based Business?

Given the broad scope of the GDPR, most U.S. businesses will be affected by its regulations. The new law will apply to any company that collects or holds data regarding EU citizens, even basic information such as a citizen's name or email address, if it is related to selling of goods or services to those individuals or to monitoring their digital activities. As a result, it arguably applies to nearly every company in the world that has any digital presence, such as a website or an app. The GDPR does not exempt smaller companies from compliance – not even for a solo proprietor.

Even if a U.S. company were to cease doing business with EU citizens to avoid having to comply with the GDPR, those efforts would likely prove fruitless. For example, if the U.S. business maintains a website that uses cookies and the site can be accessed by EU citizens, the company would still fall under the specter of the GDPR even if it's not making any sales to those customers. Alternatively, despite having no EU clients of its own, if the U.S. business has clients or customers that serve or sell to EU citizens and the U.S. business will have access to these citizens' personal data, the client or customer will likely require the U.S. company to be GDPR-compliant as a condition of winning or maintaining its business. Without taking such precautions, the client or customer risks suffering the GDPR's draconian financial penalties merely for the U.S. company's failure to comply with the regulations.

Key GDPR Provisions

CONSENTS AND DISCLOSURES

The GDPR defines "personal data" extremely broadly to include any information related to a natural person that can be used to directly or indirectly identify the person, including the person's name, email address or computer IP address. For any business that processes or stores personal data of EU citizens, any online forms and interactions with these citizens will need to be adjusted to obtain explicit consent to the gathering of personal information.

Companies will need to adhere to the following rules when collecting such personal information:

- Consent language must be clear and concise, without lengthy terms and conditions or other legal jargon.
- Consent must require an affirmative act by the individual. Having the "consent" box pre-checked or using any other form where inactivity constitutes consent is prohibited.
- Separate consents must be obtained for each different intended use of the personal data.
- The process for withdrawing prior consent must be at least as easy as the process for granting consent.
- Any third parties who will have access to the information must be identified.
- For citizens aged 16 or younger, consent from a parent or legal guardian must be obtained before collecting the child's personal information.

Any consents obtained before May 25, 2018, that fall short of the GDPR's requirements will not be "grandfathered" and will become invalid.

PROCESSORS VS. CONTROLLERS

The GDPR differentiates between data processors and data controllers. A "data processor" is a person or entity that stores or uses personal data, but doesn't exercise control over the data or dictate how the data will be processed or used. Examples of data processors include payroll companies and accountants. A "data controller" is a person or entity that controls the personal data and determines how it will be processed and for what purposes it will be used.

Under the DPA, only controllers were responsible for maintaining data privacy. While data processors will now also be subject to liability, controllers will remain potentially liable for the actions of the data processors with which they work. As such, controllers will need to be vigilant regarding their processors' compliance with the GDPR.

RIGHT TO BE FORGOTTEN AND RIGHT OF PORTABILITY

Under the GDPR, EU citizens have the "right to be forgotten" and the "right of portability." The former means that citizens have the right to require companies to delete their personal data at any time. The latter means that citizens have the right to require that a controller provide them with their personal data in a commonly used and machine-readable format, and to transmit that data to another controller without hindrance.

DATA PROTECTION OFFICER

Under the GDPR, an organization must appoint a Data Protection Officer (DPO) if its core activities consist of large-scale data processing which requires regular and systematic monitoring of EU citizens or involves processing data concerning racial or ethnic origin, personal health, sexual orientation or other sensitive information, or regarding criminal convictions or offenses. However, even if businesses aren't required to appoint a DPO, they will still likely have to devote specific, ongoing resources to ensure GDPR compliance.

DISCLOSURES FOLLOWING A DATA BREACH

The GDPR requires a company to report a data breach to the applicable governmental authorities within 72 hours of its discovery, under most circumstances. When the breach "is likely to result in a high risk to the rights and freedoms" of any affected EU citizens, the company must also inform each of the affected EU citizens about the breach "without undue delay." Communicating the information merely through a press release, social media post or announcement on the company's website will not suffice; direct correspondence with each individual affected is required.

TRANSFERRING DATA ACROSS BORDERS

The GDPR regulates how and if data about EU citizens can be transferred outside the EU's member states' borders. Essentially, to be allowed to transfer data to a country not subject to the GDPR, the business engaged in the transfer must ensure that the receiving country has been deemed to have equal or better data protection laws in place as the EU. Only a handful of countries currently meet that criteria, and the United States is not one of them. Given the ease of transporting information across borders, often with just a single keystroke or click, the consequences of transferring data without proper GDPR compliance in place could be devastating.

PENALTIES FOR BREACH

One of the most significant differences between the GDPR and the DPA is the harsh nature of the penalties that can be imposed for non-compliance. A company that fails to adhere to the GDPR's requirements can face fines up to the greater of four percent of its annual global revenue or 20 million euros.

How To Ensure Your Company is GDPR Compliant

Below are a dozen critical steps that your company should consider taking to help ensure GDPR compliance. The list is not intended to be exhaustive; more action might be required, especially once it becomes clear how the EU will enforce the GDPR after it becomes effective in May.

1. Audit your company's data. Ensure that you are aware of all data you collect or use, where the data originated, every person or entity with which the data has been shared or will be shared, and each location where it is stored.
2. Develop consent and disclosure forms that are clear and concise, without lengthy "legalese." Make sure your consent forms require an affirmative act and do not contain a pre-checked consent box or otherwise have the default result constitute consent.
3. Obtain separate consents for each different intended use of personal data and store these customer responses in a database.
4. Review all previously obtained consents to make sure they were obtained in full compliance with the GDPR's standards. In many instances, this will not be the case, and you will need to obtain new, compliant consents.
5. Make sure that the process for withdrawing consent is at least as easy as the process for granting consent.
6. For anyone aged 16 or younger, make certain to obtain consent from a parent or legal guardian before collecting personal information.
7. Disclose all third parties who will have access to the personal information.
8. Determine whether you need to appoint a Data Protection Officer. Either way, implement policies and train your staff to handle customer data in accordance with the GDPR requirements.
9. Ensure you can detect data breaches immediately and respond to and file reports regarding said breaches in the tight timeframes required by the GDPR.
10. Make sure your policies on data retention meet GDPR requirements. Adhere to the time limit for the storage of data on EU citizens, and purge the data when the purpose for which the information has been collected has been achieved.
11. If you transfer data across borders, ensure that the GDPR requirements for doing so are satisfied.
12. Make sure that any companies with which you do business that have access to your stored personal data are GDPR compliant.

If you have questions or would like to discuss the GDPR further, please contact Peter C. Spier or any of your business lawyers at Gould & Ratner, or visit www.gouldratner.com for more information.

Peter C. Spier

Partner

pspier@gouldratner.com

(312) 899-1615

Peter Spier has a diverse corporate practice, representing middle-market companies, private equity and venture capital funds and entrepreneurs, as well as emerging and established companies in the growing and dynamic gaming industry.

gould+ratner

Complex World. Practical Solutions.®

For more than 75 years, Gould & Ratner LLP has provided comprehensive legal counsel and business advice to Fortune 500 corporations, closely held businesses, financial institutions and entrepreneurs, as well as families and their businesses in litigation, real estate, corporate, tax, estate and succession planning, intellectual property, human resources and employment, environmental and related specialty fields.

222 North LaSalle Street • Suite 800
Chicago, Illinois 60601
(312) 236-3003 O • (312) 236-3241 F
www.gouldratner.com Member of LawExchange International