Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

GDPR Is Here — What If You Didn't Prepare?

By **Joseph Facciponti and Katherine McGrail** (May 24, 2018, 11:02 PM EDT)

Joseph Facciponti

Katherine McGrail

Full compliance with Europe's sweeping new data privacy law, the General Data Protection Regulation, is now required for any business that falls within the law's wide territorial scope. Yet although the GDPR was on the books for two years before its provisions became mandatory, some firms are still not fully prepared to comply with it and others might not even realize that it applies to them. Businesses that are only now waking up to the reality of the GDPR will likely not be able to make themselves compliant overnight. They must therefore prioritize their compliance efforts to mitigate potential regulatory risks as they work quickly to achieve full compliance.

What Is the GDPR Again?

The GDPR is a comprehensive European privacy law that was adopted by the European Commission in 2016 and became mandatory on Friday. The GDPR creates a series of enforceable rights that are intended to give natural persons (referred to as "data subjects") greater control over their personal data.

The GDPR defines personal data broadly as "any information" relating to an "identified or identifiable natural person." Certain "special categories" of personal data, which includes data related to race or ethnic origin, sexual orientation, political and religious beliefs, and genetic and biometric information, are entitled to additional protections under the law.

The GDPR is an EU regulation, so the terms and concepts used in it may be unfamiliar to American businesses. For example, the GDPR uses the term "processing" to generally refer to any action with respect to personal data, including the collection, use, storage, alteration, transfer, destruction, and disclosure of data. The term "controller" refers to entities that determine how and why data is processed, such as a bank that uses its customers' personal data to offer banking services, whereas the term "processors" refers to entities that process personal data on behalf of a data controller, such as a bank's third-party vendors.

The GDPR's requirements can be grouped into a few general categories:

Data Protection

The GDPR requires businesses to protect the confidentiality of the personal data they process, including by (1) adopting security safeguards, which may include encryption or masking the identity of the data subjects (pseudonymization) and (2) limiting the collection and use of data to only what is necessary to accomplish the specific goal for which the data is being processed (data minimization). Further, the GDPR requires data controllers to ensure that their data processors follow these safeguards as well.

Data Breach Notification

The GDPR requires data controllers to disclose data breaches to data privacy regulators within 72 hours and, in some circumstances, to data subjects. Likewise, processors must notify controllers of a data breach.

Limitations on Processing

The GDPR requires that data controllers have a "lawful" basis for all data processing, such as (1) the consent of the data subject, (2) where the processing is necessary for the performance of a contract with the data subject, or (3) where the data controller has a legitimate interest in the processing that is not outweighed by the data subject's rights and interests. Additional requirements apply to the processing of special categories of data and to processing that involves automated decision-making. Certain high-risk processing activities require controllers to undertake data protection impact assessments.

Transparency

The GDPR requires data controllers to provide data subjects with information that clearly explains, among other things, the data subjects' privacy rights, what personal data is being processed, by whom, the lawful basis therefor, and whether any third parties might receive it.

Data Privacy Rights

The GDPR provides that data subjects have certain rights that must be honored by data controllers upon request, including, among others, the right to have their data erased (right to be forgotten), the right to have inaccurate data corrected (right to rectification), and the right to transfer personal data from one data controller to another (right to data portability).

Limitations on Data Transfers Outside the EU

The GDPR places further restrictions on transfers of data outside of the EU, particularly to countries that, like the U.S., have been judged by the European Commission to have inadequate levels of data protection. In such cases, the GDPR requires that controllers undertake the transfer subject to certain safeguards, such as binding corporate rules for affiliated companies or certification mechanisms such as the EU-U.S. Privacy Shield Framework. If such safeguards are not available, then controllers may make transfers in specific situations based on "derogations" such as data subject consent, where the transfer is necessary to perform a contract with the data subject, or where the transfer is necessary for the establishment or defense of legal claims.

Who Must Comply With the GDPR?

The GDPR applies to entities that fall into any one of three categories. In the first instance, the GDPR applies to the processing of personal data "in the context of the activities" of an "establishment" of an organization within the EU, regardless of whether the processing occurs in the EU or not. "Establishment" is a broad concept that applies to a wide range of business arrangements and activities.

However, even if an organization is not established within the EU, it will still be caught by the GDPR if it processes the personal data of data subjects in EU where the processing activities are related "to the offering of goods or services" to such data subjects in the EU, even where no payment is sought. When considering whether goods or services are being offered in the EU, the GDPR appears to require some affirmative act by a firm, however small, to seek customers in the EU. For example, the mere accessibility of a U.S.-based company's website from the EU would not trigger the application of GDPR. However, the outcome might be different if the website affirmatively indicated that it is seeking customers in the EU, such as by accepting payment in EU currencies or providing content in EU languages.

Finally, any entity may be covered by the GDPR if it monitors the behavior of data subjects in the EU, such as tracking the internet usage of data subjects in the EU.

What Happens to Entities That Fail to Comply With the GDPR?

The GDPR empowers both data subjects and regulators to seek remedies for noncompliance. Under the law, data subjects may bring lawsuits to collect damages for any harm resulting from a violation of their rights.

With respect to regulators, the GDPR grants a wide range of enforcement powers to the data privacy regulators of each member state, including the power to carry out investigations, order entities to undertake remedial measures for deficiencies, and to impose administrative fines of up to €20 million or 4 percent of annual worldwide turnover, whichever is higher. Individual EU member states can impose additional penalties, including criminal sanctions, for noncompliance with the GDPR.

What to Do Now If You're Not Fully Compliant

Regulators in the EU might have some patience for growing pains in a company that just adopted a GDPR compliance program, but they will not look kindly on companies that have not taken any steps to comply with the GDPR at all. Companies seeking to become complaint will need to set priorities and act fast. Here are some tips.

Know Your Data

The keystone of the GDPR is personal data. Thus, an essential first step in GDPR compliance is to understand what personal data you have, where it is stored, what you use it for, and who you share it with. Carrying out a data mapping exercise helps you meet this goal by giving you a road map of your organization's data flows. And remember, the GDPR does not just cover customer data; if you have employees or agents based in the EU, their personal data is covered too.

Determine if You Have a Lawful Basis to Process Data

Once you know what personal data you and have and how you are using it, determine if you have a

lawful basis under the GDPR for your data processing activities. In many instances, this will be straightforward. If you process a customer's personal data to provide them with agreed-upon goods or services, you will typically have a lawful basis for that processing. But things become more complex if you share your customers' personal data with third parties for reasons unrelated to the services you provide to your customers (including sharing personal data with advertising and marketing companies), if you process special categories of personal data, if you use personal data to engage in automated decision-making or profiling, or if you otherwise engage in high-risk processing. In those instances, you may need to look harder at your justifications for your data processing and may also need to undertake a data protection impact assessment.

Document Your Data Processing Activities

Once you know what personal data you process, who you share it with, and the lawful basis for your processing, document this information. The GDPR requires that you keep records of your processing activities.

Update Your Privacy Policies

Another cornerstone of GDPR compliance is transparency in what you do with the personal data you collect. And a company's privacy policies are an easy way for regulators to evaluate GDPR compliance. Your privacy policies should be easily accessible, presented in plain language your data subjects can understand, and inform the data subjects of their rights and the ability to raise a complaint. Your policies should further disclose, among other things, what types of personal data you are collecting, what you are doing with it, your legal basis for processing that data, and how long you intend to keep the data.

Comply With Requests From Data Subjects

The GDPR establishes rights for data subjects, such as the right to rectification, the right of data portability, and the right of access. In most circumstances, controllers are required to promptly honor these requests. Failure to do so can lead a data subject to raise a complaint with a data privacy regulator, drawing regulatory attention to your company.

Update Your Vendor Agreements

If your company uses third-party vendors to process personal data, you must obtain "sufficient guarantees" that your vendors will safeguard the data and will comply with the applicable provisions of the GDPR. Among other things, your vendor agreements should describe the processing to be undertaken by the vendor, stipulate that your vendors are only allowed to process personal data on your instructions, and further require that the vendor will protect the confidentiality of your data. Agreements should further require the vendor to notify you of a data breach and provide you with audit rights to determine whether the vendor is complying with the terms of your agreement.

Assess Grounds for Transfers of Personal Data Outside of the EU

Transfers of personal data to third countries outside the EU are only permitted where the conditions laid down in GDPR are met. Evaluate your current transfer mechanisms to ensure they are compliant with the GDPR.

Revise Data Breach Notification Protocols

Companies should update their protocols and incident response plans to accommodate the GDPR's data breach notification requirements, which provide that controllers must notify the appropriate data privacy regulator within 72 hours of learning of the breach and, under certain circumstances, any data subjects affected by the breach.

Determine if You Must Appoint a DPO or a Representative

In certain circumstances, the GDPR requires that companies must retain or appoint additional staff or consultants to ensure compliance with the law. For example, companies must appoint a data protection officer if the company's "core activities" consist of processing operations that require "regular and systematic monitoring of data subjects on a large scale" or when processing special categories of data. Further, organizations not established in the EU may need to appoint a representative in the EU that can act on the organization's behalf with respect to data privacy regulators and data subjects.

Conclusion

Although the clock has run out for becoming compliant with the GDPR before its provisions became mandatory, companies can nonetheless demonstrate momentum toward GDPR compliance by moving quickly and prioritizing their compliance efforts.

Joseph P. Facciponti is a partner at Murphy & McGonigle PC and former cybercrime prosecutor at the U.S. Attorney's Office at the Southern District of New York.

Katherine McGrail is a partner at the firm.