GDPR: What (and Why) You Need to Know About EU Data Protection Law

by Kyle Petersen

The European Union General Data Protection Regulation (GDPR) went into effect on May 25, 2018. You have likely already heard of GDPR, but why should you care about EU law? You should care because GDPR expands the territorial scope of EU data protection laws, significantly increases the penalties for non-compliance, and is enshrouded with uncertainty. In other words, it should have your attention because: (i) organizations with no physical presence in the EU may be subject to GDPR; (ii) like U.S. anti-bribery and anti-trust laws, GDPR introduces extremely high fines – up to 4% of annual global turnover (an activist group in the EU filed complaints against Facebook and Google within hours of GDPR coming into effect seeking roughly $8 billion in fines); and (iii) it remains to be seen how strict EU data protection authorities will enforce GDPR. GDPR comes from a civil law legal system, which can be frustrating for U.S. trained attorneys to navigate. Civil law jurisdictions are historically highly regulated, but enforcement of those regulations is often inconsistent. For these reasons, you should be aware of GDPR and understand it enough to recognize when it might affect your clients.

The first thing to know about GDPR is to whom it applies. GDPR applies to organizations established outside the EU that: (i) process (as defined below) personal data of individuals located in the EU; (ii) offer goods or services to individuals located in the EU; or (iii) monitor behavior of individuals located in the EU. *See* Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, 2016 O.J. (L 119), art. 3. U.S. organizations will be subject to GDPR if they engage in these activities, despite not having a physical presence in the EU.

This article addresses key provisions of GDPR that are likely to affect U.S. organizations, particularly those in the business-to-business, or B2B, context. It also provides practical insights on achieving compliance and the challenges organizations will likely face in doing so. While it focuses on aspects that many consider to be the most concerning, this article addresses a mere fraction of GDPR. For example, in the B2C context, organizations need to have a legal basis for processing personal data, comply with GDPR's notice requirement, and be able to respond appropriately to individuals exercising their "data subject rights," all of which this article does not address but are equally important.

BACKGROUND ON EU DATA PROTECTION LAWS

Since 1995, the EU has regulated data privacy under Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 1995 O.J. (L 281) (Directive). A directive is EU legislation that requires member states to achieve a certain goal but allows each member state to implement its own laws on how to reach such goal. The Directive resulted in twenty-eight data protection laws across the EU. In an effort to keep pace with technology, offer greater protections and rights to EU citizens, and harmonize data protection laws, EU Parliament approved the final text of GDPR in 2016. Unlike the Directive, GDPR is a regulation – a binding legislative act that is enforceable as law in all EU member states. The immediate result of GDPR will be one comprehensive data protection law in the EU, instead of twenty-eight, although GDPR has several "opening clauses,"

KYLE PETERSEN is an associate attorney at Kirton McConkie.

which permit EU member states to modify certain provisions of GDPR. While many aspects of the Directive continue in GDPR, there are key differences that will affect U.S. organizations. Just how much effect GDPR will have on an organization will depend on whether that organization is considered a data controller or processor under GDPR.

CONTROLLER V. PROCESSOR

Before you worry about all of GDPR's ninety-nine articles, you must understand your client's business well enough to answer this question: is your client a controller, processor, or both? The answer to this question defines what regulatory duties your client has under GDPR.

GDPR defines controller as "the natural or legal person… which, alone or jointly with others, determines the purposes and means of the processing of personal data." GDPR, art. 4. Simply put, a controller is the person who owns or functionally controls the personal data. GDPR defines processor as "a natural or legal person…which processes personal data on behalf of the controller." *Id.* Processors take direction from controllers and do not have the right to determine the purpose for which personal data will be used.

Though the distinction may seem clear, in practice many organizations weave in and out of controller and processor roles. When making the controller-processor determination, it does not matter what an organization calls itself. Consider for example *Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT)*, Article 29 Working Party, Nov. 22, 2006. SWIFT, a global financial service provider that facilitates international money transfers, considered itself a processor and called itself a processor in all of its consumer contracts. After the September 11, 2001 terrorist attacks on the United States, the U.S Department of Treasury subpoenaed SWIFT to provide access to personal data for the purpose of monitoring financial transactions for terrorist activity.

The Belgian data protection authority (Belgian DPA) investigated SWIFT after the *New York Times* reported on the matter in 2006. The Belgian DPA ultimately found that SWIFT, despite calling itself a processor, was functionally controlling personal data, or rather, sharing personal data without permission from its

customers. The Belgian DPA found that SWIFT violated the Belgian data protection law because, as a controller of the personal data it shared with the U.S. government, it did not provide notice to, or obtain consent from, its customers as required by Belgian law. *Id*.

The SWIFT case highlights the importance of thoughtful consideration of the controller-processor classification. It also illustrates a common scenario whereby organizations act as processors and controllers with respect to different types of data (e.g., controller of human resources data but processor of payment card information).

Controller Obligations

Controllers have several obligations under GDPR. Although many requirements introduced by the Directive continue under GDPR, GDPR introduces new controller obligations that merit special attention. Of particular concern are GDPR's breach notice, third party processor, and privacy by design and default requirements.

Breach Notice

GDPR's breach notice requirements are what many consider to be the most troublesome addition, primarily due to a sweeping definition of what constitutes a breach. GDPR defines personal data breach as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed." GDPR, art. 4.

GDPR adopts the breach notice requirement developed in the United States, a familiar concept to many U.S. attorneys. However, unlike state requirements in the U.S., which generally only apply to unauthorized access or acquisition, GDPR broadens the definition of a breach to include alteration, destruction, or loss of personal information. By way of example, a ransomware attack not involving the extraction of personal information would not generally trigger U.S. state breach notice requirements but could trigger GDPR breach notice requirements if there is a loss of personal information (i.e., an organization's inability to access its personal information).

Article 33 provides that

> [i]n case of a personal data breach, the controller shall without undue delay and where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority…unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.

Id. art. 33.

In addition to notifying the supervisory authority, an organization must also notify the data subject if the personal data breach "is likely to result in a high risk to the rights and freedoms of [the data subject]." *Id*. art. 34.

Organizations face several challenges with GDPR's breach notice requirement. First, organizations will likely not fully understand the extent of a breach within seventy-two hours of becoming aware of it but will be required to submit a report to a government authority – a report that may not accurately describe the breach. Such report could potentially be produced in class action litigation in the United States. Next, when is an organization considered to have become "aware" of the personal data breach? Finally, the exception to notifying the supervisory authority – if the breach is unlikely to result in a risk to the rights and freedoms of natural persons – will understandably lead to internal debates on the necessity of notification.

Third Party Processors

Article 28 requires that any processing carried out on behalf of a controller must be governed by a contract, and such contract must obligate the processor to:

- process personal data only on documented instructions from the controller;
- ensure confidentiality;
- implement appropriate security measures;
- assist the controller with its obligations to comply with certain provisions of GDPR;
- delete or return personal information upon request; and
- provide information necessary to demonstrate compliance with its obligations.

Id. art. 28. Article 28 poses a challenging task for organizations that outsource processing activities (e.g., cloud storage, payment processors, marketing communications, etc.). To comply, organizations will need to update their contracts (or put contracts

in place) with vendors that process EU personal data. While updating a standard form agreement with GDPR specific language is a relatively simple task, the real challenge is identifying current vendors that process EU personal data, locating those contracts, and explaining to vendors why you need them to take on additional burdens or liability in the middle of the term with no additional compensation.

Vendors, especially those with no nexus to the EU, will likely question why they must assist the counter party with its GDPR compliance. In many cases, U.S. vendors will be unfamiliar with GDPR. Organizations will need to carefully determine what contracts need to be updated and be prepared to explain to vendors the reason why. Whether you advise controllers or processors, watch out for language that appears GDPR-related but is too broad or narrow (i.e., the contract introduces obligations not required under Article 28 or obligations that do not meet the standards set forth in Article 28).

Privacy by Design and Default

Prior to GDPR, organizations complied with global data protection laws via privacy policies, contractual terms, registrations, etc. For the first time in the privacy arena, GDPR requires organizations to take one step further and develop products with privacy in mind. This will require different departments within an organization to work together to develop GDPR-compliant policies, procedures, and systems simultaneously with product development. This concept is known as privacy by design.

Article 25 provides that

> [t]aking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing.

Id. art. 25.

One challenge an organization may face here is whether its products or systems are capable of complying with certain requirements under GDPR. For example, GDPR grants several rights to data subjects, including the right to erasure and data portability. *Id.* art. 17, 20. That is, individuals have the right to request that a controller delete their personal information (right to erasure) or export it in a machine-readable format for their own personal use (data portability).

Many existing technology systems were not designed to delete data or export it in machine-readable format. Updating such

systems can be costly and time consuming. However, organizations may consider the cost, available technology, and risks to data subjects when deciding whether to undertake substantial engineering efforts to restructure products and systems. In other words, technical and organizational measures implemented by Facebook may not be appropriate for your client's organizaiton.

In addition to privacy by design, GDPR requires privacy by default. Article 25 further provides that "[t]he controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed." *Id*. art. 25. Privacy by default refers to procedures and settings an organization implements. It requires that organizations (i) only collect personal information for a specified purpose; (ii) retain the minimum amount of personal information necessary; and (iii) retain such personal information only as long as necessary.

Organizations will struggle to implement privacy by design and default without knowing key information about the data it collects. Specifically, an organization should know what type of data it collects (human resources, marketing, etc.), where it stores data (on-site servers, cloud, etc.), how long data is kept, and how it is used. This process is known as mapping. Data mapping will help organizations develop internal GDPR-compliant policies and procedures.

Processor Obligations

Under the Directive, only controllers had direct compliance obligations. This is not the case under GDPR. GDPR introduces several new requirements on processors and exposes them to substantial penalties and claims. While processors have fewer obligations than controllers, they will face significantly increased risk under GDPR. Key obligations on processors include the duties to notify the controller of a breach and to implement appropriate security measures.

Breach Notice

Article 33 requires processors to "notify the controller without undue delay after becoming aware of a personal data breach." *Id*. art. 33. However, a processor's obligation with respect to a data breach will likely not stop at notifying the controller. As noted above, if the controller is GDPR compliant, its contract with a processor will require the processor to assist the controller with its breach notice obligations. Therefore, processors will not only be required to notify the controller of a breach but can also expect to be contractually obligated to provide other information about the breach that will assist the controller with its compliance obligations under Article 33. A processor's failure to notify the controller of a data breach not only exposes the processor to penalties under GDPR, it may also result in a breach of contract.

Security Measures

Article 32 provides that the "processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk," including pseudonymisation and encryption of personal data, the ability to ensure the ongoing confidentiality, and the ability to restore the availability and access to personal data following a technical event. *Id*. art. 32. Accordingly, processors and controllers have the same obligation to implement appropriate security measures. Under the Directive, controllers were responsible for ensuring that processors implemented such measures. GDPR now places that responsibility on processors as well.

When advising on what constitutes appropriate security measures, what may be appropriate for one processor may not be appropriate for another. Processors (and controllers) have some flexibility in making this determination because GDPR allows processors to consider the state of the art, costs of implementation, nature, scope, context, and purposes of processing, as well as the risk to data subjects.

As noted above, controllers should still contractually obligate processors to implement appropriate security measures, which means a failure of a processor to do so will result not only in a breach of contract, but also a violation of GDPR.

CONCLUSION

GDPR is here to stay and will likely become the global standard for data privacy. In today's data-driven world, you should understand GDPR well enough to recognize when it might impact your client's business. While GDPR introduces several obligations that could potentially affect U.S. organizations, you should pay particular attention to whether your client is a controller, processor, or both. Making that determination will identify what obligations your client has under GDPR. Complying with those obligations will protect your clients from claims and substantial penalties under GDPR.