Shumaker

DECEMBER 18, 2018 | PUBLICATION

Client Alert: The European Union's General Data Protection Regulation Becomes Effective

SERVICE LINE

Corporate, Tax and Transactions

RELATED ATTORNEYS

Regina M. Joseph

MEDIA CONTACT

Wendy M. Byrne
wbyrne@shumaker.com

On May 25, 2018, the European Union's ("EU") long-talked about and broadly applicable General Data Protection Regulation ("GDPR") became effective, bringing sweeping changes to how organizations must handle personal data belonging to those located within the EU. The regulation is not just for European business, but impacts every organization that offers goods and services to individuals located within the EU. In the age of global e-commerce, the GDPR impacts many American businesses, too many of whom have yet to take any steps towards becoming compliant. This Client Alert is a primer on the applicability of the GDPR and necessary steps to work towards compliance.

In plain English, the GDPR is designed to afford greater protections for personal data belonging to persons located within the EU. It aims to accomplish this by imposing requirements on organizations to be transparent with data subjects about how they collect, use, share and transfer personal data, and requiring organizations to take technological and organizational measures to protect the rights of data subjects, such as pseudonymisation and encryption of personal data. The GDPR also affords individuals located within the EU with several data rights, including the right to access the information an organization holds, rectification or correction of such information, erasure, and the right to withdraw consent, the right to object to a processing activity, the right to data portability, and the right to file a complaint with a supervisory authority where an organization is not complying with the GDPR.

What is personal data?

Personal data is broadly defined under the GDPR as any information relating to an identified or identifiable natural person ("data subject"), by reference to an identifier such as a name, identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.[1] The GDPR is structured around two central roles, that of the (1) data controller and (2) data processor. A data controller is any natural or legal person, public authority, agency or other body which, alone or jointly with others is tasked with determining the purposes and means of processing personal data.[2] A data controller is usually the business that makes the determination about what information to collect from the customer, how long the information will be stored, and how the information will be used in the business.

The term "processing" is defined as any operation or set of operations performed on personal data, including by means of automation, including collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.[3] A data processor is any natural or legal person, public authority, agency or other body responsible for processing personal data on behalf of the controller.[4] Data processors are usually service providers that work on behalf of the data controller and provide services such as data storage, web hosting, marketing, or payment card processing services.

What triggers applicability of the GDPR?

The regulation is applicable to an organization if any one of the following applies: (1) the organization, regardless of location, collects personal data in conjunction with offering goods or services to persons (no payment of money is required) where such person is located within the EU, (2) the organization monitors the behavior of persons located within the EU, or (3) the organization is located within the EU and collects and processes personal data of data subjects within the context of commercial activities.[5] Thus, something as simple as maintaining a website where individuals from within the EU can enroll to receive a free promotional newsletter, or tracking web traffic that include European users, are activities sufficient to subject an organization to the GDPR. Significantly, the GDPR is not just applicable to EU citizens or residents, but rather anyone physically located within the EU.[6]

My organization falls into one of the three categories mentioned above, where do I begin?

If you suspect your organization may be subject to the GDPR, the first step is to understand how your organization collects, uses, stores, shares and transfers personal data that it assembles. Commissioning an experienced vendor to construct a data map is one of the best ways to capture the manner in which data flows throughout the organization and can be used to identify GDPR concerns. A data map is a snapshot of how an organization uses data at a particular point in time. Often a data mapping exercise will involve reviewing information governance and data retention policies in conjunction with interviews of personnel that actually do the collection and use the personal data, which will enable the organization to better identify gaps between how data is practically managed and the organization's documented policies.

What are the compliance requirements?

Every processing activity concerning personal data must be lawful.[7] Article 6 of the GDPR outlines each lawful basis for processing. Most commonly, controllers will rely on consent from the individual or the processing will be necessary for compliance with a legal obligation, such as a contract.[8] Where processing is based on consent, certain rules apply. Generally, consent must be given in the context of a written declaration, which is clearly distinguishable from other manners, easily accessible, and written in clear and plain English.[9] Consent must also be freely given under the circumstances.[10]

Depending upon the types of information collected and the purposes for processing, the processing activity may be prohibited. Special categories of personal data, such as ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data health data and data concerning a person's sex life or sexual orientation cannot be processed, except for the limited exceptions detailed in Article 9.[11] The processing of special categories of personal data also triggers the requirement that the controller or processor appoint a representative located in the EU for purposes of communicating with the data supervisory authority and data subjects to comply with the GDPR.[12]

In addition to securing a lawful basis for processing information, the controller is required to provide disclosures to data subjects in conjunction with the requirement for transparency. Controllers are required to provide certain information to individuals when the data is collected from the data subject to enable that data subject to make an informed decision about whether he or she wants to provide their personal data to the controller.[13] Where personal data is not obtained directly from the individual, a few additional disclosures are required by Article 14.[14] Often these disclosures are included in the organization's privacy policy.

Controllers are also tasked with implementing appropriate technical and organizational measures to protect the rights of data subject.[15] The GDPR instructs controllers to take into account the state of the art, cost of implementation, the nature, scope, context and purposes of processing and the risks, varying likelihood and severity of the rights and freedoms o
f natural persons posed by the processing in making a determination about the appropriate technical and organizational measures to implement.[16]

For processing activities that are not occasional, are large scale, concern processing of special categories of data, personal data relating to criminal convictions and offenses and processing that is likely to result in a risk to the rights and freedoms of natural persons, the controller or processor is required to designate a personal representative in the EU, which is established in a EU member state where the data subjects whose personal data is processed or whose behavior is monitored, are located.[17] This required representative will be addressed by the supervisory authorities and data subjects on all issues relating to the processing to ensure compliance with the GDPR.[18]

The GDPR imposes a requirement on the controller to have written contracts in place with its processors that handle personal data, which must contain several specific provisions detailed in Article 28.[19] These requirements are generally aimed at ensuring that processors conduct their processing activities in strict compliance with the controller's instructions, subject to confidentiality and in compliance with the GDPR.[20] Processors wishing to engage with another processor are also required to have a written contract in place with such subprocessors, which contains at least the same level of protections that are imposed by the controller on the processor and the processor must ensure that any subprocessor will meet the requirements of the GDPR.[21] Notably, the Processor is required to remain liable to the controller for any failure by the subprocessor to fulfill its obligations.[22]

In addition to having a contract detailing the parties' obligations, the GDPR imposes substantial record keeping obligations under Article 30.[23] Controllers are generally required to keep track of the purposes of processing, a description of categories of data subjects and categories of personal data, categories of recipients of the personal data, transfers of personal data outside the EU, time limits for which the personal data will be stored, and a general description of the technical and organizational measures implemented for protecting the rights of data subjects.[24] Processors are generally required to keep details on whose behalf the processor is processing the data, the categories of processing carried out for each controller, information on transfers of personal data outside the EU, and a general description of the organizational and technical

measures implemented to protect data rights.[25] An exception to the record keeping obligation exists where an organization employs less than 250 persons, is occasional, does not involve special categories or data and is not likely to result in the risk to rights and freedoms of data subjects.[26]

Does my organization need to appoint a Data Protection Officer ("DPO")?

Under circumstances where a controller and processor engage in processing operations that by virtue of their nature, scope or purpose, require regular and systematic monitoring of data subjects on a large scale or involve large scale processing of special categories of personal data and personal data relating to criminal convictions and offenses, the organization may be required to appoint a data protection officer.[27] The data protection officer is tasked with informing and advising the controller or processor and the employees that carry out the processing activities of their obligations under the GDPR and other EU laws.[28] The data protection officer is also required to: (1) monitor compliance with the GDPR and other EU laws; (2) monitor compliance with the controller or processor's policies in relation to the protection of personal data; (3) train staff involved in processing operations; (4) monitor audits; (5) provide advice with respect to data protection impact assessments; (6) cooperate with the supervisory authority; and (7) to act as the contact point with the supervisory authority on issues relating to processing.[29] Data protection officers are to act independently from the organization in carrying out their duties and are insulated from termination, except as specifically noted in Article 38.[30]

What are the Penalties under the GDPR?

Non-compliance is subject to stiff penalties. The GDPR affords data subjects with the right to lodge a complaint with a supervisory authority of an alleged infringement of such data subject's rights.[31] A data subject can also maintain a legal action against a controller or processor.[32] Article 82 of the GDPR provides the right to compensation where the data subject has suffered damage as a result of an infringement on his or her rights.[33] In addition, the GDPR provides for administrative penalties that can range as high as the greater of (1) €20,000,000 euros; or (2) 4% of the total worldwide gross revenue for the previous year.[34]

How can Shumaker help?

Enlisting the assistance of experienced legal counsel in GDPR matters can be extremely helpful in traversing this complicated European regulation. Shumaker, Loop & Kendrick, LLP has experienced lawyers that are regularly advising businesses of all sizes concerning GDPR compliance issues. For additional information, contact Regina Joseph at rjoseph@shumaker.com, (800) 444-6659, ext 1435, or Matthew Spaulding at mspaulding@shumaker.com, (800) 444-6659, ext. 1455.

---

[1] GDPR, Article 4(1).

[2] GDPR, Article 4(7).

[3] GDPR, Article 4(2).

[4] GDPR, Article 4(8).

[5] See GDPR, Article 3.

[6] See GDPR, Article 3(2).

[7] See GDPR, Article 6.

[8] See GDPR, Article 6(1)(a) & (b).

[9] GDPR, Article 7.

[10] Id.

[11] GDPR, Article 9.

[12] See GDPR, Article 27(2)(a)

[13] See GDPR, Article 13.

[14] See GDPR, Article 14.

[15] GDPR, Article 25

[16] GDPR, Article 25(1).

[17] GDPR, Article 27(2)(a).

[18] GDPR, Article 27(4).

[19] GDPR, Article 28.

[20] See GDPR, Article 28(3)(a).

[21] GDPR, Article 28(2) & (4).

[22] GDPR, Article 28(4).

[23] GDPR, Article 30.

[24] GDPR, Article 30(1).

[25] GDPR, Article 30(2).

[26] GDPR, Article 30(5).

[27] See GDPR, Article 37(1).

[28] GDPR, Article 39.

[29] GDPR, Article 39.

[30] GDPR, Article 38(3) & (6).

[31] GDPR, Article 77.

[32] GDPR, Article 79.

[33] GDPR, Article 82.

[34] GDPR, Article 83.