insights

SHUMAKER
Shumaker, Loop & Kendrick, LLP

A Newsletter from Shumaker, Loop & Kendrick, LLP | Summer 2017

Privacy Compliance Driven by the European Union

By Regina M. Joseph

and Matthew C. Spaulding

Data is the core of the information age, just as land was essential to the agrarian age and iron ore fueled the industrial age and steel production. Big data is the raw material of deep learning by artificial intelligence, as well as the raw material of social media giants. Big data is, of course, information about you and me--the purchases we make, our choices for health care, choices for music, and choices for other myriad minutia.

The privacy of personal data is rapidly becoming a primary concern. Most countries have new laws on the books or in process. In an interconnected world, an act of ecommerce could implicate laws beyond the sender's immediate geographic borders. For multi-national companies, processing of human resources data and sending it cross-border (either internally or through vendors and supply chain partners) might trigger multiple laws that protect personal data.

In an interconnected world, an act of ecommerce could implicate laws beyond the sender's immediate geographic borders.

Many hope that compliance with the European Union's new General Data Protection Regulations ("GDPR") will serve as a gold standard for many countries. The GDPR and its penalties become effective on May 25, 2018.

Companies with any hint of personal data affecting the EU are scrambling to get a handle on exactly where the data is, what the data is, what is being done with it, where it is going, who will see it, who is responsible for it, and whose consent is required.

They are performing this data mapping because the GDPR penalties will be substantial—ranging as high as the greater of 20,000,000 euros *or* 4% of total worldwide annual turnover for the preceding year.

What triggers applicability of the GDPR?

The GDPR is designed to reinforce the data protection rights of individuals and to facilitate the free flow of personal data by virtue of a more uniform regulation adopted across the EU. 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.[1] 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.[2] 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.[3]

The GDPR is triggered for a data controller or processor located within the EU if personal data of individuals located in the EU is being processed in relation to any commercial activity, regardless of whether the processing activity occurs inside or outside of the EU.[4] The GDPR is triggered for a data controller or processor located outside of the EU where it engages in any one of the following activities: (1) offering goods or services to individuals located within the EU ("EU data subjects"), (2) monitoring the behavior of EU data subjects while such individuals are located inside the EU, or (3) employing individuals in the EU.[5] It is important to note that the applicability of the GDPR is not limited to EU citizens, but rather anyone physically within the EU.[6]

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

A company that may be subject to the GDPR is well-served by understanding how data is collected, used, stored and transferred within and outside the organization. Commissioning an experienced vendor to construct a data map is one of the best ways of capturing the manner in which data flows throughout the organization and can be used to confirm whether the organization is subject to the GDPR. The data map may also be used to identify data risk within the organization, prioritize issues for GDPR compliance, and to expose any gaps between how data is practically managed and the organization's documented policies.

What are compliance requirements?

Controllers are required to assess the nature, scope, context and purposes of processing and the risks, likelihood and severity for the rights and freedoms of natural persons and then to implement appropriate technical and organizational measures to ensure and demonstrate that it is processing personal data in accordance with the GDPR.[7] A controller is required to conduct a similar analysis each time it makes a determination about a means of processing personal data and must design technical and organizational measures for that process to meet the safeguards required by the regulation.[8] By default, the controller is also tasked with installing technical and organizational measures to ensure that only the personal data necessary to satisfy the specific purpose of the processing is actually processed, a principle that applies to the amount of personal data collected, the extent of processing, the period of time the personal data is stored, and its accessibility, including implementing measures to prevent unauthorized access.[9]

In addition to design requirements, controllers and processors are also required to implement technical and organizational measures to ensure an appropriate level of security after assessing the cost of implementation, the nature, scope, context and purposes of the processing and the likelihood and severity of risk to the rights and freedoms of natural persons.[10] Controllers and processors are required to implement measures to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services, the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident, and a process for regularly testing, assessing and evaluating the effectiveness of the technical and organizational measures to ensure security of the processing.[11]

The GDPR also imposes substantial record keeping requirements on both controllers and processors. Controllers and, where applicable, their representatives are required to maintain records of processing activities, including the name and contact details of the controller, the purposes of processing, a description of categories of data subjects and categories of personal data, categories of recipients to whom the personal data will be disclosed, any transfers of personal data to a third country or an international organization, time limits

for erasure of the different categories of data and a general description of technical and organization security measures.[12] Processors and their representatives, if applicable, are tasked with maintaining records of name and contact details of the processor or processors of each controller on whose behalf they process, categories of processing carried out on each controller's behalf, any transfers of personal data to a third country or international organization and a general description of the technical and organization security measures.[13] There is an exception to both of these record keeping requirements for controllers and processors where an organization employees fewer than 250 people unless the processing being carried out is likely to result in a risk to the rights and freedoms of data subjects, is not occasional or includes special categories of data (e.g., racial or ethnic origin, political opinions, religious or philosophical beliefs).[14]

Under the GDPR, controllers have information disclosure obligations to EU data subjects once the controller obtains personal data.[15] Requirements vary depending upon whether the controller actually collects the personal data from the EU data subject versus when such personal data is not obtained from the data subject.[16] Generally, the controller is required to provide contact details about itself; the purpose, legal basis for and legitimate interests pursued by the processing; recipients or categories of the personal information; details about any intended transfer of the personal data outside the EU and international organization; information regarding how long the data will be stored; the EU data subject's right to access, rectify, erase, restrict, object, and withdraw any consent given and the right to data portability among other information.[17] These requirements are designed around the principle of processing personal data, which include lawfulness, fairness and transparency, purpose limitations, data minimization, accuracy, storage limitations, integrity and confidentiality, and accountability.[18]

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

The GDPR requires the controller or processor to designate a DPO where its core activities require regular and systematic monitoring of EU data subjects on a large scale or involve processing a large scale of special categories of data, such as those about criminal convictions or offenses, race, and political or religious beliefs.[19] Unfortunately, the GDPR does not define what might constitute "large scale processing." In lieu of any official guidance or commentary on the GDPR from the EU Data Protection Board ("Data Protection Board"), the Article 29 Data Protection Working Party ("WP 29"), an advisory group on data protection and privacy to the EU Commission, has suggested that organizations consider, in evaluating whether their processing is on a "large scale," such factors as the number of data subjects affected, the volume and range of data and data items processed, the duration of the data processing activity, and the geographical extent of the processing activity. [20]

The term "core activities" is defined in Recital 97 of the GDPR as the "primary activities that do not relate to the processing of personal data as ancillary activities."[21] WP29 has suggested that primary activities may be considered as "key operations necessary to achieve the controller's or processor's goals."[22] An example provided in WP29's guidance is a hospital, whose core activity is to provide healthcare - a hospital could not provide healthcare effectively without processing health data, including an individual's health records.[23] Thus, WP29 concludes processing data should be construed as one of the hospital's core activities.[24]

If it is determined that the organization must appoint a DPO, the individual chosen must have expert knowledge of data protection law and practices and be able to fulfill the tasks and responsibilities specified in the GDPR.[25] The requisite level of expert knowledge is to be determined based on the data processing operations being carried out and the protection required for the data processed.[26] There is no requirement that an organization appoint a DPO from outside the organization.[27] A DPO may be a staff member or may fulfill the tasks on the basis of a service contract.[28] The DPO may fulfill other tasks and duties outside of his or her DPO role, as long as such other tasks and duties do not result in a conflict of interest.[29] Regardless of who is selected as the DPO, the GDPR makes it abundantly clear that the DPO must be able to perform their job tasks in an independent manner, requiring that controllers and processors ensure that the DPO does not receive any instructions concerning the exercise of the DPO's responsibilities under the GDPR.[30] Moreover, a DPO cannot be dismissed or penalized for performing his/her duties as the DPO and must directly report to the highest management level of the controller or processor organization.[31]

Controllers and processors also have responsibility for insuring that the DPO is involved promptly and properly regarding all issues that relate to the protection of personal data.[32] The controller and processor are required to support the DPO in performing the tasks of the DPO and by providing resources necessary to carry out such tasks, including access to personal data and processing operations and maintaining the DPO's expert knowledge.[33] Reasonable access must be afforded by the controller and processor to the DPO for EU data subjects so that the DPO may be contacted by such subjects about the processing of their personal data and to exercise their rights under the GDPR.[34]

Chapter 8 of the GDPR sets forth remedies, liability and penalties under the GDPR. Article 77 provides the data subject the right to lodge a complaint with a supervisory authority in a particular Member State of his or her habitual residence, place of work or place of the alleged infringement. Article 79 affords each data subject the right to an effective judicial remedy where the data subject's rights under the Regulation have been infringed. Article 79 also provides that a proceeding against a controller or processor is to be maintained in the courts of the Member State where the controller or processor has an establishment or in courts of the Member State where the data subject has his or her habitual residence. Article 82 provides the right to compensation to any person who has suffered damage as a result of an infringement of the Regulation from a controller or processor for the damage suffered. Most importantly, this private right of action is in addition to the administrative fines discussed above.

In conclusion, the EU has demonstrated its commitment to enforcing privacy violations. For example, in May 2017, the European Commission fined Facebook the equivalent of $122 million for privacy-related nondisclosures made in its merger review documentation submitted in 2014 for its WhatsApp acquisition. Separately, the Italian antitrust authorities levied a 3 million euro fine on WhatsApp for allegedly requiring users to agree to share their personal data with Facebook. Although these fines are hefty, they pale to potential GDPR penalties.

For additional information, contact Regina Joseph at rjoseph@slk-law.com, ***1-800-444-6659, ext. 435, or Matthew Spaulding at*** mspaulding@slk-law.com, ***1-800-444-6659, ext. 1455.***

Shumaker works collaboratively with an established vendor to provide a full service international solution, including data mapping and analysis.

FOOTNOTES

[1] GDPR, Article 4(7).

[2] GDPR, Article 4(2).

[3] GDPR, Article 4(8).

[4] *See* GDPR, Article 3.

[5] GDPR, Article 3(2).

[6] *See* GDPR, Article 4(1); GDPR, Recital 2.

[7] GDPR, Article 24(1).

[8] GDPR, Article 25(1).

[9] GDPR, Article 25(2).

[10] GDPR, Article 32.

[11] *Id.*

[12] GDPR, Article 30.

[13] *Id.*

[14] *Id.*

[15] *See* GDPR, Articles 13 & 14.

[16] *Id.*

[17] *Id.*

[18] GDPR, Article 5.

[19] GDPR, Article 37(1).

[20] Article 29 Data Protection Working Party, *Guidelines on Data Protection Officers ('DPOs')*, WP243 rev.01, Section 2.1.3, page 8, available at: http://ec.europa.eu/justice/data-protection/index_en.htm.

[21] GDPR, Recital 97.

[22] Article 29 Data Protection Working Party, *Guidelines on Data Protection Officers ('DPOs')*, WP243 rev.01, Section 2.1.2, page 6, available at: http://ec.europa.eu/justice/data-protection/index_en.htm.

[23] *Id.*

[24] *Id.*

[25] GDPR, Article 37(5).

[26] GDPR, Recital 97.

[27] GDPR, Article 37.

[28] GDPR, Article 37(6).

[29] GDPR, Article 38(6).

[30] GDPR, Article 38(3).

[31] *Id.*

[32] GDPR, Article 38(1).

[33] GDPR, Article 38(2).

[34] GDPR, Article 38(4).