WILLKIE FARR & GALLAGHER LLP

NEW YORK WASHINGTON HOUSTON PARIS LONDON FRANKFURT BRUSSELS MILAN ROME

CLIENT MEMORANDUM

New European General Data Protection Regulation Officially Adopted

May 10, 2016

AUTHORS

Daniel K. Alvarez | **Marc J. Lederer**

On May 4, 2016, the new European General Data Protection Regulation (the "GDPR") was published in the *Official Journal of the European Union*, the final step marking the official adoption of the GDPR throughout the European Union. It goes into effect later this month, and all companies to which the law applies must come into compliance by May 25, 2018.

As we reported in our December 17, 2015 Client Memo, the GDPR will impact organizations across the globe that do business in Europe or even with citizens of the European Union. It establishes a number of new data protection requirements with respect to doing business with EU-resident individuals, such as new privacy notice requirements, new contractual requirements for service provider contracts, new data breach notification rules, new rights for individuals and new accountability obligations. Noncompliance with the GDPR could result in substantial monetary penalties.

In this memo, we highlight some of the key requirements in the GDPR that companies need to consider as they begin to review their existing data collection, use and sharing practices and make the necessary changes to come into compliance with the GDPR.

GDPR Requirements

Who Must Comply with the GDPR

Unlike the data protection directive that has been in place in the EU since 1995,[1] the GDPR will apply to any "data controller"[2] that "processes"[3] the "personal data"[4] of any individual EU resident ("data subject")[5] in the context of offering the data subject goods or services,[6] regardless of where the data controller is located. As such, many businesses that have no physical presence in the EU may be subject to the GDPR simply by receiving personal data from EU data subjects. With respect to having an online presence, factors to be considered when determining whether a website is offering goods or services to data subjects that are resident in the EU include: (a) the accessibility of the website or an email address in the EU (or that of an intermediary); (b) the language and currency used; and (c) the mentioning of customers or users who are in the EU.

The GDPR also governs efforts to monitor the behavior of EU data subjects, insofar as the data subjects' behavior takes place within the EU. Monitoring would include Internet tracking and profiling of data subjects, particularly with respect to making decisions concerning data subjects or analyzing or predicting their personal preferences, behaviors and attitudes.

---

1 Directive 95/46/EC[3], OJ L 281, 23.11.1995.

2 A "data controller" is the natural or legal person, public authority, agency or any other body that alone or jointly with others determines the purposes, conditions and means of the processing of personal data; where the purposes, conditions and means of processing are determined by EU law or Member State law, the controller or the specific criteria for his nomination may be designated by EU law or by Member State law. Unlike in the federal data protection laws in the United States, data controllers are not just limited to certain regulated sectors, such as the financial or health industries.

3 "Process" or "Processing" means any operation or set of operations that is performed upon personal data or sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, erasure or destruction.

4 "Personal data" means any information relating to a data subject. Anonymous data would not be covered under the GDPR since it cannot be used to identify an individual. However, the GDPR contains some protections for pseudonymous data, since it could potentially be used to identify an individual if associated with other data.

5 "Data subject" means an identified natural person or a natural person who can be identified, directly or indirectly, by means reasonably likely to be used by the data controller or by any other natural or legal person, in particular by reference to an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

6 The GDPR does not apply to the processing of personal data for purely personal or household activities without a connection to a professional or commercial activity.

Finally, the GDPR also applies both directly and indirectly to "data processors."[7] Data processors can be held directly responsible under the GDPR for noncompliance with applicable rules and data protection obligations (data security, data impact assessments, recordkeeping, appointment of data protection officers, international transfer rules, etc.). And data processors are indirectly governed by the GDPR inasmuch as the GDPR requires that data controllers must select data processors that can provide sufficient data protection in accordance with the GDPR, and then imposes a number of requirements for contracts between data controllers and data processors.[8]

Privacy Notices

The GDPR mandates certain disclosures in a privacy notice. Alongside the typical disclosures, such as the identity of the data controller, the purposes of the data processing, and the categories of recipients of the personal data, the GDPR requires disclosures that may be new to some data controllers. Some of these disclosures include: (a) retention period; (b) contact details for the data protection officer (if any); (c) the right to access, rectification or erasure; (d) the right to object and the right of portability; (e) the right to lodge a complaint with a supervisory authority; and (f) information regarding possible data transfers to other countries or international organizations.

Data Breach Notification

The GDPR requires that as soon as the data controller becomes aware that a data breach has occurred, it should notify an EU supervisory authority without undue delay and, where feasible, within 72 hours.[9] The data controller is also required to notify the affected individuals without undue delay if it determines that the breach could adversely affect those individuals. A breach should be considered as adversely affecting the personal data or privacy of a data subject where it could result in, for example, identity theft or fraud, physical harm, significant humiliation or damage to reputation.

Data Protection Officers

The GDPR requires that data controllers and data processors appoint a data protection officer where the processing is carried out in the public sector, the processing is carried out in the private sector by a large enterprise (250 employees or more), or the entity's core activities, regardless of the size of the enterprise, involve processing operations that require

---

7 A "data processor" is the natural or legal person, public authority, agency or any other body that processes personal data on behalf of the data controller.

8 These requirements include terms dealing with: (a) the right of subcontractor approval by the data controller; (b) details regarding the processing purposes, types of personal data, categories of data subjects and duration of the processing; (c) the deletion or return of personal data to the data controller following the end of services; (d) the allowance of auditing or inspection by the data controller or its representative; (e) assistance provided to the data controller with respect to data breach analysis and reporting; and (f) provisions concerning confidentiality and data security.

9 If data breach notification cannot be made to an EU supervisory authority within 72 hours, then an explanation of the reasons for the delay should accompany the notification when made.

regular and systematic monitoring. Such data protection officers should be experts in this field and should be able to perform their duties in an independent manner.

Consent

The GDPR calls for consent to be given by a clear, affirmative act that is freely given, specific, informed and unambiguous, such as by a written statement, including by electronic means, or an oral statement. This could also take the form of ticking a box that has not been pre-ticked or another statement or conduct that clearly indicates consent. *Silence or inactivity should not constitute consent.*

Consent will often be viewed as not freely given in the context of an employer-employee relationship because there is a perceived "significant imbalance" between the positions of the data subject and the controller. Parental consent is required for the processing of personal data of a data subject under 16 years of age. The GDPR allows for individual EU nations to lower the age for required parental consent, but in no case may it be lower than 13 years of age.

With respect to direct marketing activities, the GDPR explicitly gives data subjects "the right to object at any time to processing of personal data concerning him or her for such marketing." Once that right has been invoked, "the personal data shall no longer be processed for such purposes."

Subject Access, Right to Object, Right to Rectification, Portability and Erasure

The GDPR provides data subjects with several new and expanded rights. In particular:

- Data subjects have a right to obtain information about the processing of their personal data in a timely manner and generally free of charge;
- Data subjects have an expanded right to object to certain processing of their personal data;
- Data subjects have the right to correct inaccurate personal data about them;
- Data subjects have the right to have their personal data transferred to other parties in a structured, commonly used and machine-readable format; and
- Data subjects have the right to have their personal data erased and/or forgotten under certain conditions.

Enforcement and Penalties

Although the GDPR creates a single European data privacy law to replace the data privacy directive and individual national implementations of that directive, enforcement of the GDPR will lie primarily with the national data protection authorities – and their enforcement powers will be significantly expanded. In particular, monetary penalties under the GDPR can be substantial, with administrative fines authorized of up to a maximum of 20 million euros or 4% of total worldwide global turnover of the prior financial year, whichever is higher.

Other GDPR Topics

Other subjects dealt with in the GDPR include: (a) restrictions on profiling; (b) a requirement to maintain records relating to data processing; (c) conducting data impact assessments when data processing presents certain risks; (d) a duty to implement appropriate technical and organizational measures to safeguard and protect data; and (e) approved mechanisms for international data transfers, such as model contract clauses and binding corporate resolutions.[10]

Next Steps

Two years may seem like plenty of time, but May 25, 2018 will be here quickly, and with potential penalties for non-compliance of the size contemplated by the GDPR, there is no reason to delay. Those persons and entities, wherever located, doing business in the EU or with EU individuals will want to use that time wisely to determine whether the GDPR applies to them and, if so, what they need to do to come into compliance. Many parties that would be data controllers and data processors under the GDPR will need to review and revise their privacy notices, vendor contracts and internal policies, among other things. In addition, certain businesses may need to appoint data protection officers and obtain consents from data subjects, among other obligations. We expect that there will be additional guidance from EU privacy regulators over the next two years that will help businesses understand how to better comply with this new regulation. We will continue to monitor developments and keep you apprised as appropriate.

If you have any questions regarding this memorandum, please contact Daniel K. Alvarez (202-303-1125; dalvarez@willkie.com), Marc J. Lederer (212-728-8624; mlederer@willkie.com) or the Willkie attorney with whom you regularly work.

Willkie Farr & Gallagher LLP is an international law firm with offices in New York, Washington, Houston, Paris, London, Frankfurt, Brussels, Milan and Rome. The firm is headquartered at 787 Seventh Avenue, New York, NY 10019-6099. Our telephone number is (212) 728-8000 and our fax number is (212) 728-8111. Our website is located at www.willkie.com.

May 10, 2016

---

[10] The EU-U.S. safe harbor is no longer an approved mechanism for personal data transfer into the United States from the EU as explained in our March 3, 2016 Client Memo and in our February 2, 2016 Client Memo.