

CLIENT MEMORANDUM

T Minus One Year (and Counting): The EU General Data Protection Regulation Is Set to Take Effect in May 2018 – Are You Ready?

May 25, 2017

AUTHORS

Daniel K. Alvarez | **Dr. Christian Rolf** | **Henrietta de Salis** | **Rita D. Mitchell** | **Alex J. Moyer** | **Marc J. Lederer**

In May 2016, the European Union (“EU”) adopted the General Data Protection Regulation (“GDPR”) to establish more uniformity over privacy and data security regulation throughout the EU, and gave regulated entities two years to comply.¹ That effective date of the GDPR – May 25, 2018 – is officially now only one year away. This may seem like plenty of time, but GDPR imposes some onerous and detailed requirements. Organizations whose data processing activities fall within its scope should consider the impact of GDPR on their businesses and prepare for its implementation right away, if they have not done so already.

We have previously reported – in our [December 17, 2015 Client Memo](#) and our [May 10, 2016 Client Memo](#) – on the breadth and depth of GDPR. Since then, we have gained some insight into the issues that are most pressing for organizations faced with the GDPR compliance burden, and there have been a number of further developments, including additional actions by EU member states, and guidance issued by EU data protection authorities (“DPAs”) and the Article

¹ Regulation (EU) 2016/679 (“GDPR”).

T Minus One Year (and Counting): The EU General Data Protection Regulation Is Set to Take Effect in May 2018 – Are You Ready?

Continued

29 Working Party (“WP29”).² This memo proceeds in two parts: first, we provide a brief overview of the GDPR, including its scope, substantive requirements, and potential penalties for non-compliance (some of which may serve primarily as a reminder for those who have read our previous memos); and second, we briefly highlight some of the recent developments that we are monitoring.

The GDPR

Scope. The GDPR’s scope is significant, covering all data processing activities involving the personal data of an EU citizen, regardless of where the data is collected, where the processing takes place, or where the data controller is located. In other words, companies that have no physical presence in the EU may be subject to the requirements of the GDPR if they happen to collect data from an EU citizen. Almost all of the GDPR’s requirements apply to companies regardless of their size and amount of data processing.³

Requirements. To help understand what GDPR could mean for your organization, the following is a list of some key considerations:

- **Privacy Notices:** The GDPR likely will affect the way companies provide notice to customers and website visitors. It includes a longer and more detailed list of information that must be provided than what was previously required under EU law. In particular, Article 13 requires that data subjects receive clear, concise, and easily-understood information regarding, among other things, the data that is being processed, the purposes for which the data is being processed, and the identity of the data controller. These notices must also include information about data subjects’ rights (discussed below) and how to exercise them. Companies should thus examine their privacy notices, both for content and presentation, to be sure they comply with the GDPR.
- **Consent:** The GDPR appears to raise the bar regarding the primary means of ensuring that processing is lawful – the consent of the data subject – and organizations should assess their methods of obtaining data subjects’ consent to ensure sufficiency under the GDPR. The GDPR requires that consent be “freely given, specific, informed and unambiguous.”⁴ Data subjects must also be able to withdraw their consent at any time with respect to continued processing. Furthermore, the GDPR places the burden on controllers to establish the adequacy of consent.

² WP29 is the independent European Union Advisory Body on Data Protection and Privacy, comprised of representatives from each of the EU Member States, the European Data Protection Supervisor, and the representative of the European Commission. See European Commission, *Article 29 Working Party*, http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083.

³ The requirements to designate a data protection officer and to conduct a data protection impact assessment are triggered only if the controller’s data processing activities are “regular” or “large-scale,” or otherwise present a high risk to data subjects. GDPR, Arts. 35(3) & 37(1). However, these concepts are not defined, leaving some uncertainty as to the precise triggers for these requirements.

⁴ GDPR, Art. 4(11).

T Minus One Year (and Counting): The EU General Data Protection Regulation Is Set to Take Effect in May 2018 – Are You Ready?

Continued

- **Data Subjects' Rights:** The GDPR provides data subjects with a number of rights regarding their personal data, including, among others, the rights of access, rectification, erasure, data portability, and objecting to certain types of processing. Some of these will not be new for organizations that do business in the EU, but all covered organizations should review their data processing practices to ensure their ability to respond to a request from a data subject to exercise her rights.
- **Security:** Organizations must review their existing security practices and procedures in light of the strictures of the GDPR. In particular, GDPR requires organizations to implement an “appropriate level of security” for the personal data they collect and hold, including protection against unauthorized or unlawful processing and accidental loss, destruction, or damage. The “appropriate level of security” takes into account a number of factors, among them the state of the art; the costs of implementation; the nature, scope, context, and purposes of the processing; and the risks and severity of harm to the data subjects, and may include pseudonymization and encryption.
- **Data Protection Impact Assessment:** Organizations that intend to engage in processing that is likely to result in high risk to the rights of the data subject must conduct a data protection impact assessment (“DPIA”), in consultation with their data protection officer (“DPO”), prior to the processing. When a DPIA finds that a high risk exists, the GDPR requires the company to consult and cooperate with the local DPA, who may then provide guidance and instruction.
- **Breach Notification:** The GDPR introduces data breach notification requirements for the first time in EU law. Under the GDPR, a data controller must notify the appropriate national DPA – for example, the Information Commissioner’s Office (“ICO”) in the UK – of a breach *within 72 hours* of becoming aware of it. The GDPR also requires notifications to individuals (subject to a few exceptions), prescribes the form of notifications, and mandates certain record keeping requirements. Companies, now more than ever, must be prepared to respond to a breach, and should frequently review and update incident response protocols.
- **Service Providers:** The allocation of responsibilities between controllers and processors under the GDPR may affect companies’ relationships with their vendors and service providers. For example, there are a number of data protection stipulations that are required to be in contracts with service providers. Companies are thus encouraged to review agreements with service providers and revise them accordingly. Additionally, the GDPR places obligations directly on service providers, such as to implement appropriate technical and organizational measures. This means that all companies that handle EU data subjects’ personal data must assess and maintain appropriate security practices.
- **Cross-Border Transfer:** The GDPR does not represent a substantial change from the current EU Data Protection Directive in terms of its restrictions against cross-border transfer. Perhaps its most significant change is that it allows for the use of model contract clauses without prior approval from a DPA. Despite requiring only minor changes, the implementation of the GDPR presents an opportunity for companies to reexamine their

T Minus One Year (and Counting): The EU General Data Protection Regulation Is Set to Take Effect in May 2018 – Are You Ready?

Continued

practices and legal mechanisms for transferring data from the EU and enhance them by, for example, bolstering their notice and consent procedures or obtaining certification under the EU-U.S. Privacy Shield Framework.

- **Data Protection Officers:** One of the most-discussed requirements in the GDPR is the requirement to designate a DPO to oversee processing operations for those companies whose core activities consist of processing special categories of personal data (e.g., racial or ethnic origin, political opinions, and health information) or involve large-scale, systematic monitoring of data. In some cases, this is not a new requirement – some EU countries already require appointing a DPO in certain circumstances. But the GDPR’s EU-wide mandate covering organizations that perform large-scale, systematic monitoring has forced many companies to scramble to find somebody to fill the role.

Penalties. Monetary penalties under the GDPR should incentivize organizations to focus on compliance. The GDPR authorizes administrative fines of up to of €20 million or 4% of total worldwide global revenues of the prior financial year, whichever is higher.

Recent Developments

WP29 Guidance. While not having the effect of law, the WP29’s guidance documents are often relied upon by DPAs, such as the UK’s ICO and others, and organizations should incorporate any relevant WP29 guidance into their GDPR compliance efforts. To date, the WP29 has adopted guidelines, with FAQs, on the following GDPR topics: (1) data portability; (2) DPOs; and (3) identifying a controller or processor’s lead supervisory authority.⁵ In addition, the WP29 has stated that it intends to produce new guidance on the following GDPR topics: (1) administrative fines; (2) high-risk processing and DPIAs; (3) certification; (4) profiling; (5) consent; (6) transparency; (7) notification of personal data breaches; and (8) tools for international transfers. Organizations should be on the lookout for each such WP29 publication.

DPA Guidance. Likewise, some of the individual DPAs have engaged in consultations on specific topics to provide guidance. For example, the ICO earlier this year undertook a consultation with respect to the principle of consent under the GDPR, and issued guidance to “give more detailed, practical guidance for UK organisations on consent under the GDPR.”⁶ These guidance documents, as with those issued by the WP29, provide helpful insight into the way that regulators are approaching these new requirements.

⁵ WP29 invited comments on these guidelines and is considering the responses received. See http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083.

⁶ Information Commissioner’s Office, *Consultation: GDPR consent guidance* (Mar. 31, 2015), <https://ico.org.uk/media/about-the-ico/consultations/2013551/draft-gdpr-consent-guidance-for-consultation-201703.pdf>.

T Minus One Year (and Counting): The EU General Data Protection Regulation Is Set to Take Effect in May 2018 – Are You Ready?

Continued

Other EU Laws. Despite the fact that one of the goals of the GDPR is greater uniformity in privacy and data security law across the EU, various GDPR articles allow member states to issue specifications to the GDPR.⁷ Germany has recently passed such a law, which will come into effect together with the GDPR.⁸ Other EU member states are expected to follow suit. Organizations should also consider the implications that the GDPR may have for other recordkeeping obligations, such as those under the Markets in Financial Instruments Directive,⁹ the Market Abuse Regulation,¹⁰ and anti-money laundering rules, among other requirements.

Conclusion

With the compliance date for the GDPR being only one year away, businesses subject to this new regulation need to begin preparing for compliance, if they have not already. As you move forward, Willkie's Cybersecurity & Privacy team can help you assess and navigate the GDPR's impact on your business. We will continue to monitor the implementation of the GDPR over the coming year and beyond, and keep you informed.

If you have any questions regarding this memorandum, please contact Daniel K. Alvarez (202-303-1125, dalvarez@willkie.com), Dr. Christian Rolf (+49 69 79302 151, crolf@willkie.com), Henrietta de Salis (+44 20 3580 4710, hdesalis@willkie.com), Rita D. Mitchell (+44 20 3580 4726, rmitchell@willkie.com), Alex J. Moyer (202-303-1280, amoyer@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 25, 2017

Copyright © 2017 Willkie Farr & Gallagher LLP.

This memorandum is provided by Willkie Farr & Gallagher LLP and its affiliates for educational and informational purposes only and is not intended and should not be construed as legal advice. This memorandum may be considered advertising under applicable state laws.

⁷ See, e.g., GDPR, Art. 88.

⁸ Data Protection Amendment Act regarding Regulation (EU) 2016/679 and transformation of Directive (EU) 2016/680 (Data Protection Amendment and Transformation Act EU (DSAnPUG-EU)).

⁹ Directive 2014/65/EU.

¹⁰ Regulation (EU) No 596/2014.