Client Update
GDPR – 12 Months to Go – 10 Steps You Should Consider Now

LONDON
Jane Shvets
jshvets@debevoise.com

Chris Garrett
cgarrett@debevoise.com

Robert Maddox
rmaddox@debevoise.com

FRANKFURT
Dr. Thomas Schürrle
tschuerrle@debevoise.com

Fritz Popp
fpopp@debevoise.com

PARIS
Pierre Clermontel
pclermontel@debevoise.com

Fanny Gauthier
fgauthier@debevoise.com

NEW YORK
Jeremy Feigelson
jfeigelson@debevoise.com

Jim Pastore
jjpastore@debevoise.com

WASHINGTON, D.C.
Luke Dembosky
ldembosky@debevoise.com

INTRODUCTION

There is just one year to go until the General Data Protection Regulation (the "GDPR") comes into full force on 25 May 2018, replacing the existing EU Data Protection Directive (the "Directive"). Data privacy and cybersecurity have been increasingly in the news and on regulators' agendas, and there is no reason to believe this trend will diminish. In this client update, we set out ten key issues businesses should consider now to prepare for the changes the GDPR will bring.

1. Determine if your company is subject to the GDPR

Like the Directive, the GDPR will apply to all companies that have a presence in the European Union, but it also significantly expands the territorial scope of the EU data protection regime. Specifically, even companies with no EU presence will have to comply with the GDPR if they process personal data of "data subjects" who are in the EU in connection with (1) "offering of goods or services" to data subjects (no payment required); or (2) "monitoring" of the data subjects' behaviour online, for example, for the purposes of subsequent profiling. The "offering of goods or services" prong of the GDPR's territorial scope is very fact-specific and requires careful consideration of a non-EU company's business model vis-à-vis customers located in the EU, including whether that company's online presence is likely to be perceived as envisaging serving individuals located in the EU.

2. Consider hiring a Data Protection Officer

The GDPR will require companies whose core activities require large-scale "regular and systematic monitoring" of data subjects or large-scale processing of their sensitive data to appoint data protection officers ("DPOs"). Some EU data protection authorities, such as the CNIL in France, have gone even further and

strongly recommend that all companies that process EU personal data appoint DPOs to ensure GDPR compliance. Identifying a qualified person to serve as a DPO may be a challenging task, given the extensive expertise and capabilities expected of this role. A 2016 study estimated that the GDPR would create 28,000 vacant DPO positions, and companies that must (or want to) appoint a DPO should begin the recruitment process without delay. Companies that are not obliged to appoint a DPO, but wish to appoint a person responsible for data protection compliance, should consider creating a position with a title other than a "DPO" to avoid unnecessarily imposing mandatory obligations of the DPO on that individual.

3. Update fair processing and privacy notices

The GDPR aims to increase transparency about how personal data is handled, expanding the types of information that organisations have to provide to individuals to ensure fair and transparent processing of their data. Privacy notices or policies published on websites and elsewhere may need to be updated to include information about, among other things: (1) data retention periods; (2) safeguards relating to data transfers outside the EU; (3) contractual or statutory consequences of refusal to provide personal data; and (4) contact information of the company's DPO, where applicable. That information must be provided in "concise … and easily accessible form, using clear and plain language"; data protection jargon and overly technical language should be avoided. Although providing additional information may not be overly onerous in and of itself, identifying existing deficient notices that require updating may be a significant task for some businesses.

4. Assess consent

Consent is one of the bases for legitimately processing personal data under the Directive and will remain one under the GDPR. The GDPR, in contrast to some Member States' existing regulations, toughens the definition of a valid consent and casts doubt on whether much of pre-GDPR consent-based personal data processing will remain valid.[1] If your company relies on data subjects' consent for processing their data, make sure that those consents remain valid post-GDPR, including that they are (1) specific to the particular processing activity; (2) voluntary; and (3) active (requiring a positive step rather than inaction on the data subjects' part).

---

[1] *See, e.g.*, D&P Client Update, *UK Information Commissioner's Office Issues GDPR Consent Guidance: What Business Should Know and Do*, 7 March 2017; *available at* http://www.debevoise.com/insights/publications/2017/03/uk-information-commissioners-office-issues?wb48617274=4A20E446.

5. Consider conducting a data protection impact assessment

Data protection impact assessments will become mandatory under the GDPR where large-scale processing of sensitive personal data or data subjects' profiling are involved. These are, in essence, data privacy risk assessments, aimed to determine whether a company is adequately addressing its data protection risks and to remediate as warranted. As with the appointment of DPOs, organisations should consider whether conducting an impact assessment is advisable as a tool for ensuring GDPR compliance even if it is not strictly required under the GDPR.

6. Implement an incident response plan

The GDPR introduces, for the first time, a pan-EU data breach notification obligation, requiring companies that suffer qualifying personal data breaches to notify relevant EU supervisory authorities and, in some cases, affected individuals. Notifications must be made without undue delay and in any event within 72 hours, a time frame that, practically speaking, means that companies subject to the GDPR need to have a cyber incident response plan ("IRP") in place before a breach occurs. Organisations subject to the GDPR should also set out in their IRPs the process for determining whether a breach has to be notified and, if so, the procedure for making the notifications.

7. Review and update data processing agreements

Companies should review existing contracts with third parties that process personal data on their behalf to ensure that they are valid post-GDPR. Such contracts should include a range of requirements on data processors, including assistance with and reporting of data breaches, technical and organizational measures the data processor must undertake to safeguard the data, and audit rights.

8. Be prepared to comply with new and enhanced individual rights

The GDPR enshrines a host of new individual rights—including the rights to data erasure ("right to be forgotten") and data portability and the right not to be subject to automated decision-making (for example, profiling)—and expands existing rights, for example the right to receive, on request, information about the processing of an individual's personal data. Many of the new and expanded individual rights aim to increase individuals' ability to control the way in which their personal data is handled. As such, companies should be prepared for the possibility that they would be receiving a significantly higher number of requests and complaints from data subjects. It is most prudent to prepare for that ahead of time by setting out policies and procedures for responding to such requests and complaints (or reviewing policies and procedures already in place).

9. Identify your lead supervisory authority

Under the GDPR, one data protection supervisory authority will take the lead on investigating data protection issues that implicate several EU Member States for companies established in the EU. Although more guidance on this subject is anticipated, it is likely that, for companies operating in more than one EU Member State, the lead supervisory authority would be the one covering the jurisdiction of the company's headquarters and/or the centre of the corporate decision-making. EU data protection authorities have explicitly discouraged "forum-shopping" for lead supervisory authorities, but it remains worthwhile for companies to consider who its lead supervisory authority would be and whether more than one supervisory authority could credibly claim that title. For companies that are at higher risk of scrutiny (*e.g.*, those that process large quantities of personal data), it is then prudent to establish good working relationships with the lead supervisory authorities and ensure that they keep up to date with those authorities' guidance and expectations.

10. Train staff

With all the new provisions that GDPR introduces, it is essential to ensure that company staff—and in particular the employees dealing with individuals' personal data—are appropriately trained. In most cases, that training must extend not just to the DPO or the employees specifically tasked with data protection compliance functions, but also IT, Legal, Human Resources, Marketing, and other functions whose activities inadvertently can put companies at risk of violating the GDPR.

CONCLUSION

While the GDPR is still 12 months away from coming into force, organisations that are or may be subject to its jurisdictions should spend that time to prepare, including by implementing the steps outlined above. We expect regulators to be unsympathetic to those who are not compliant by 25 May 2018, given that the final text of the GDPR has been available since 2016 and has been widely discussed and analysed since then. The time to consider GDPR's impact on your business, and take the appropriate steps, is now.

* * *

Please do not hesitate to contact us with any questions.