LATHAM&WATKINS

Client Alert Commentary

Latham & Watkins Data Privacy, Security & Cybercrime Practice 24 May 2016 | Number 1972

Europe Counts Down to the General Data Protection Regulation

Businesses have two years to comply with Europe's new privacy regime.

Today, after more than four years of debate, the General Data Protection Regulation (GDPR, or the Regulation) enters into force. The GDPR will introduce a rigorous, far-reaching privacy framework for businesses that operate, target customers or monitor individuals in the EU. The Regulation sets out a suite of new obligations and substantial fines for noncompliance. Businesses need to act now to ensure that they are ready for when the Regulation becomes enforceable after the expiry of a two-year transition period, *i.e.*, from 25 May 2018.

The regulatory climate

The GDPR will replace and repeal Data Protection Directive 95/46/EC (DPD, or the Directive), that underpins Europe's current data protection regime. The GDPR aims to respond mainly to two main problems: First, EU Member States have individually transposed the Directive into national law, and the 29 different sets of implementations have increasingly diverged, creating a patchwork of data protection laws (and accompanying compliance issues) across the EU. Second, rapid changes to technology, and specifically the increasing reliance of online applications and services on personal data to market and sell goods, have caused new challenges for the protection of data subjects.

Plus ça change

While the Regulation introduces significant new and strengthened obligations for businesses, most core concepts remain. The definition of personal data — data from which a living individual is identified or identifiable, directly or indirectly — is retained and accompanied with additional examples (location data and online identifiers) where data might be considered as identifiable. The GDPR expands the scope of sensitive personal data to include genetic and biometric data, but retains much of the DPD's definition. Whilst the GDPR maintains the distinction between data controllers (which determine the purposes and means of processing personal data) and data processors (which process the data on behalf of the controller), it allocates compliance obligations more equitably between them.

Despite this ostensible familiarity, businesses must respond to many changes now to ensure future compliance once the two-year transition period expires.

Will this affect your business?

The GDPR is ambitious and broad in scope, highlighting its purpose of protecting data subjects in the EU from adverse data processing, regardless of where the data controller may be established. As such, the GDPR will apply to:

- **Any organization established in the EU:** If your business is established in the EU and processes personal data as part of its business, it will have to comply with the GDPR. The Court of Justice of the European Union (CJEU) specified the criteria for "establishment" in its 2015 *Weltimmo* decision, confirming that an organization can be established through "stable arrangements" in the EU, where it exercises "any real and effective activity — even a minimal one." The GDPR's broad scope applies regardless of whether the organization is a data controller or a data processor (as mentioned above, unlike the DPD regime, the GDPR attaches additional direct obligations to data processors). The Regulation also applies regardless of whether the entity actually processes personal data within the EU. So, for example, the GDPR would apply even if an Irish business stores its data on the cloud via servers in Singapore. The presence of a branch, subsidiary or even a single representative within the EU may be enough to trigger the application of the GDPR.

- **Any non-EU organization offering goods or services to EU data subjects:** If your business is not established in the EU but offers goods or services to EU data subjects, the business will have to comply with the GDPR. The threshold for what constitutes offering goods and services is still somewhat nebulous, but merely having an online presence which can be accessed by EU data subjects will likely not rise to the level of mandatory compliance — the organization must actively "envisage" offering the goods and services, for example by using an EU language or currency and mentioning EU users.

- **Any non-EU organization monitoring the behavior of EU data subjects:** If your business tracks EU data subjects to profile their online behavior — especially with the goal of analyzing or predicting the data subject's attitudes, personal preferences and behavior — then the GDPR will apply to your business. The language will certainly catch online behavioral advertising networks, but the definition is broad and would cover any app that monitors location and E-Health technology.

What next?

The GDPR has such a broad scope that, according to a 2015 Ovum study, two-thirds of businesses expected that the GDPR would force changes in their European business strategy.[1] Non-EU organizations must assess whether they could be considered established in the EU even if their activities are minimal.

- **How do I make sure my non-EU business doesn't fall under the GDPR?:** First, ensure that you have no establishment in the EU. Second, make sure that you are not targeting or monitoring EU users. If EU users can access your site, do not specifically target or mention EU users, and consider making payment in EU currencies like Euros and Sterling impossible. Businesses may want to consider geo-blocking EU users for absolute certainty until they are sure their business is in compliance.

- **What happens to non-EU entities which fall under the GDPR?:** Non-EU entities which fall under the GDPR must appoint a representative in the EU and should comply with the guidance set out further below. Only limited exemptions apply to this obligation. The designated representative may be subject to enforcement proceedings and liable for any breach by the non-EU entity in the event of noncompliance by the non-EU controller or processor.

Impact

If the GDPR will apply to your business, you have two years to examine and update your business practices to ensure compliance. The risks of noncompliance are severe: under the GDPR, regulators can impose fines of up to €20 million or 4% of a corporate group's total annual worldwide turnover, whichever

is higher. In particular, businesses should take the following key steps to ensure compliance with critical areas of the GDPR:

A. Monitor B2C business practices

Businesses should first consider their B2C practices to ensure compliance:

- **Conduct a data protection audit:** If your organization is subject to the GDPR, you must fully understand from the outset how data is collected, processed, stored, used and transferred. The GDPR in principle requires that data may only be processed for the purpose for which it is collected. By fully mapping data flows and integrating such planning into future acquisitions or restructuring, businesses can more easily ensure compliance with the GDPR.

- **Examine processing grounds:** The Regulation is explicit that businesses must have a valid processing ground in each and every instance of data processing:

  - **Consent:** A data subject's consent must be "*freely given, specific, informed and unambiguous"* and, if consent is given in a document that deals with other matters, consent must be easily distinguishable from the rest of the document. The GDPR is clear that "*silence, pre-ticked boxes or inactivity should not therefore constitute consent*" and that "*when the processing has multiple purposes, consent should be given for all of them*." This will require many businesses to review their standard terms and conditions, existing consumer contracts and privacy policies.

  - **Consent from children:** Consent given by a child will only be valid if it is authorized or given by that child's guardian. The requirement applies to children under the age of 16 (though Member States may lower this to as young as 13 years old). If your organization targets children, ensure that proper parental consent mechanisms are in place, including verification processes.

  - **Legitimate interests:** Data can still be processed if the processing pursues the company's legitimate interests. Such interests include processing for direct marketing purposes, the prevention of fraud or transferring data within a group for internal purposes (though the GDPR's restrictions on international data transfers still apply — see below). Businesses should note that the legitimate interests ground will only be valid when the fundamental rights and freedoms of an individual data subject do not override the organization's legitimate interests. The GDPR also provides that codes of conduct should include guidance on legitimate interests, so members of trade associations or industry bodies should take care to comply with any additional requirements.

  - **Other grounds:** The GDPR does not significantly alter other common grounds of processing, such as processing for the performance of a contract or to comply with legal obligations.

- **Update privacy policies:** The GDPR provides that privacy policies and notices should include additional content requirements but also should "*be written in a concise, transparent, intelligible and easily accessible form, using clear and plain language*." This is harder than it may sound: CNN reported last year that users would need to be educated to at least the level of a second-year university student to understand the disclaimers in the privacy policies of several large online businesses, and an oft-cited Carnegie Mellon study from 2008 estimated that the average person would require 76 working days to read all of the privacy policies he or she encounters in a year. Yet companies can, for instance, engage with new formats to clarify their privacy practices. The UK's Information Commissioner's Office (ICO) has recommended:

- Layered notices (simplifying complex information up-front, and allowing users to delve deeper)
- Just-in-time notices (to gain consent at critical data processing junctures — though note that this will limit data processing to the processing ground given at the time)
- Videos (which generally allow for less legalese and clearer communications)
- Privacy dashboards

Large organizations should also consider working with their internal communications or public relations teams to craft unambiguous messages without losing legal substance, and sophisticated organizations can test privacy policies in focus groups to generate evidence of compliance and ensure messages are clear.

B. Monitor internal business practices

The GDPR will significantly impact businesses' internal data storage and transfer practices, and organizations will need to fundamentally reassess their data processing policies to ensure compliance with the Regulation.

- **Data processors:** Unlike the DPD, the GDPR imposes significant obligations directly on data processors, exposing data processors to enforcement actions for noncompliance. Data processors should note the stringent requirements for sub-processing (which requires the consent of the data controller and which will need to be met whenever data processing is sub-contracted), implementing appropriate security measures (including a positive obligation to ensure integrity and confidentiality) and the requirement to appoint a data protection officer if the core processing activities involve regular and systematic monitoring or the processing of sensitive or criminal data on a large scale. Practically, data processing agreements should be updated to include details of the nature and purpose of processing as well as specific obligations in the Regulation that are more extensive than those in the DPD, including prior consent for sub-contracting.

- **Pseudonymous data:** The GDPR expressly addresses the status of pseudonymous data (*e.g.*, medical data that is key coded for clinical studies). The Regulation actively encourages data controllers to adopt pseudonymization in its provisions on lawful processing, general obligations and security, stating that this approach "*can reduce the risks to the data subjects concerned and help controllers and processors to meet their data protection obligations.*" The GDPR requires organizations to have implemented processes to ensure privacy by design and suggests that pseudonymization should be considered to ensure data minimization and data security obligations are met.

- **Data transfers:** In the wake of the CJEU's ruling in the S*chrems* case — which spelled the end of transatlantic data sharing under the Safe Harbor regime — organizations will be increasingly aware of the importance of data protection principles in international data transfers. To an extent, the GDPR does not change much in comparison to today's practice: adequacy decisions and EU Model Clauses which the European Commission approved will remain in force. However, the GDPR also contains provisions that will assist businesses. In particular, transfers based on EU Model Clauses no longer need to be notified to or authorized by local data protection authorities, which will lift some of the administrative burden that exists today in many EU countries. Further, the use of binding corporate rules for intragroup transfers is specifically mentioned, and the GDPR details what information must be included and the procedure for approval.

C. Establish compliant accountability processes

The GDPR enshrines the notion of accountability for data controllers, which gives rise to specific obligations on controllers to implement policies and other documentation to demonstrate how they will comply with their obligations, and to be transparent and forthcoming about such obligations.

- **Record keeping:** Organizations are required to maintain a record of processing activities which includes, for example, the purposes of the data processing, categories of data and relevant retention periods. If organizations are considering new data processing activities, they may be required to complete a privacy impact assessment (PIA) in order to identify, and protect against, privacy noncompliance risks. The PIA is required for any "high risk" processing (such as large-scale profiling or processing of sensitive data), with risk measured against the likelihood of the processing to infringe on a person's rights and freedoms. Data processors in particular are required to maintain records of all data processing activities even if the processor does not deal directly with the personal data, which may affect cloud and hosting services in particular. Under certain requirements, there is an exception for processors that employ fewer than 250 people.

- **Appointment of Data Protection Officer (DPO):** Organizations must appoint a DPO in some cases, particularly when they engage in large-scale processing of personal data or the large-scale regular and systematic monitoring of data subjects, or where obliged to by local law. DPOs are the cornerstone of the accountability regime. The DPO should report to the highest levels of management and advise them on the implementation of the Regulation. DPOs should be involved in training staff on data protection issues, and should be the first point of contact for the appropriate supervisory authorities. Group companies can appoint a single DPO, who can be an employee or an external contractor.

- **Establish processes for dealing with data subjects:** The GDPR has maintained and strengthened rights such as subject access and the right to object. The GDPR also mentions the right to be forgotten and adds the right to data portability and certain rights to restrict processing. Not only should businesses update privacy policies to clearly set out these rights, but they should also ensure that internal processes are in place to facilitate such requests (given breach of the accountability obligations, *i.e.* not being able to demonstrate how you comply with the GDPR, attracts the maximum fines). DPOs or counsel should coordinate with IT teams about the rights of erasure and data portability, as these may need to be technically built into existing systems.

D. Invest in infrastructure

The GDPR continues to require adequate security measures to protect personal data.

- **Establish robust security processes:** Organizations are required to implement appropriate technical and organizational measures to protect the data that they process, and also to ensure that this obligation flows through contractual provisions with data processors and vendors. The GDPR provides that organizations must establish procedures for regular testing and evaluating the effectiveness of technical and organizational measures. The Regulation also encompasses business continuity in the concept of security — including the obligations to ensure information integrity and availability, as well as restoring access to data in the event of a physical or technical incident.

- **Breach notification:** The Regulation introduces a general regime for personal data breach notifications. Under this regime, data processors are obliged to report personal data breaches to data controllers. Controllers must maintain report breaches that are likely to result in a risk to the rights and freedoms of individuals to their supervisory authority without undue delay to the supervisory

authorities and, where feasible, within 72 hours of discovering such a breach. If the 72-hour deadline is not met, the breach notification must include a justification for the delay. Data controllers must also directly inform the affected data subject without undue delay if a breach "*is likely to result in a high risk to the rights and freedoms*" of that data subject. However, direct notification to the data subject will not be required if the data controller implements technical protections (such as encryption), takes subsequent measures to ensure that the breach is unlikely to be repeated, or if the communication would require disproportionate effort. The GDPR's breach notification provisions underscore the need for effective data security.

Next steps

From 25 May 2018, businesses that operate, target customers or monitor individuals in the EU will be subject to new obligations under the GDPR. In the interim transition period, data controllers and processors alike must scrutinize their business practices and policies and put together a comprehensive plan to take steps to achieve compliance. The first stage will be ensuring clear accountability for data protection matters, board level recognition of the possible fines and a strong governance structure to ensure that the business will be in compliance by the end of the two-year transition period.

If you have questions about this *Client Alert*, please contact one of the authors listed below or the Latham lawyer with whom you normally consult:

Gail Crawford
gail.crawford@lw.com
+44.20.7710.3001
London

Lore Leitner
lore.leitner@lw.com
+44.20.7710.4785
London

This *Client Alert* was prepared with the assistance of Calum Docherty, Trainee Solicitor in the London office.

You Might Also Be Interested In

Political Agreement on European Data Protection Regulation

How to Prepare for the New European Privacy Law? (webcast)

Endnotes

[1] Data Privacy Laws: Cutting the Red Tape, a Q3 2015 study by Ovum, available on the Internet at this link.