HUNTON& WILLIAMS

February 2016

Overview of the EU General Data Protection Regulation

Background

- **The existing law:** Current EU data protection law is based on Directive 95/46/EC (the "**Directive**"), which was introduced in 1995. Since that time, there have been significant advances in information technology, and fundamental changes to the ways in which individuals and organisations communicate and share information. In addition, the various EU Member States have taken divergent approaches to implementing the Directive, creating compliance difficulties for many businesses.
- **The changes:** The EU's legislative bodies have reached a political agreement on an updated and more harmonised data protection law (the "**Regulation**"). The Regulation will significantly change EU data protection law, strengthening individual's rights, expending the territorial scope, increasing compliance obligations and expanding regulator enforcement powers.

  The formal adoption is expected in Spring 2016, with the Regulation applying from Spring 2018. Organisations will have two years to implement changes to their data protection compliance programmes, business processes, and IT infrastructure to reflect the Regulation's new requirements.

Impact of the Regulation on Businesses

Key:  **This change is broadly positive for most businesses**  **This change is broadly negative for most businesses**  **This change is broadly neutral for most businesses**

Some concepts will change: The Regulation will introduce ***a number of new concepts and approaches***, the most significant of which are outlined below. The Regulation is also designed to be more future-proof and forward looking than the Directive, and as technology-agnostic as possible.

Some concepts will stay the same: ***Many of the existing core concepts under the Directive will remain unchanged.*** For example, the concepts of personal data, controllers and processors are broadly similar in both the Directive and the Regulation. These concepts are not addressed further below.

Increased enforcement powers: Currently, fines under Member State law vary, and are comparatively low (e.g., the UK maximum fine is £500,000). The Regulation will significantly increase the ***maximum fine to €20 million, or 4% of annual worldwide turnover***, whichever is greater. In addition, national data protection supervisory authorities will be co-ordinating their supervisory and enforcement powers across the Member States, likely to lead to a more pronounced enforcement impact and risk for businesses.

Greater harmonisation: The Regulation introduces a single-legal framework that applies across all EU Member States without the need for national implementation. This means that businesses will face a ***more consistent set of data protection obligations*** from one EU Member State to the next, which should aid overall compliance. However, harmonisation will not be complete and some differences will persist across the EU Member States.

Expanded territorial scope: Non-EU businesses will be subject to the Regulation if they: (i) offer goods or services to EU residents; or (ii) monitor the behaviour of EU residents. Many non-EU businesses that were not required to comply with the Directive ***will be required to comply with the Regulation***.

Consent, as a legal basis for processing, will be harder to obtain: Under the Regulation, individuals' consent must be freely given, specific, informed and unambiguous. Consent may not be valid if it is bundled with other matters, part of the general terms of conditions, or there is a "clear imbalance" between the parties. Organisations will be required to demonstrate that consent was

given. Mere acquiescence (e.g., failing to un-tick a pre-ticked box) does not constitute valid consent under the Regulation. Businesses that rely on consent to process personal data will need to carefully review their existing practices.

The risk-based approach to compliance: The Regulation acknowledges a risk-based approach to compliance, under which businesses would bear responsibility for assessing the degree of risk that their processing activities pose to individuals. ***Low-risk processing activities face a reduced compliance burden.*** On the other hand, documented ***data protection impact assessments*** will be required for high-risk processing activities. These compliance steps will need to be integrated into future product cycles.

The 'One-Stop Shop': Currently, a Data Protection Authority ("DPA") may exercise authority over businesses established in its territory or otherwise falling within its jurisdiction. Under the Regulation, where a business is established in more than one EU Member State, the supervisory authority ("SA") of the main establishment of the business will act as the lead authority for data processing activities that have an impact throughout the EU and will co-ordinate its work with other SAs. In addition, each SA will have jurisdiction over complaints and possible violations of the Regulation in their own Member State.

Data protection by design and by default: Businesses will be required to implement data protection ***by design*** (e.g., when creating new products, services or other data processing activities) and ***by default*** (e.g., by implementing data minimisation techniques). They will also be required to perform data protection impact assessments to identify privacy risks in new products.

Data Protection Compliance Programs — Internal processing records and Data Protection Officer: Organisations will have to implement and be able to demonstrate to the SA that they have comprehensive data protection compliance programmes, with policies, procedures and compliance infrastructure. For example, instead of registering with a SA, the Regulation will require businesses to ***maintain a record*** of processing activities. Also, organisations must appoint a data protection officer ("DPO") where (1) they are a public authority or body; (2) the core activities of the controller or processor require regular and systematic monitoring of individuals on a large scale; (3) the core activities of the controller or processor include processing certain types of data on a large scale, including data relating to criminal convictions and offences; or (4) required by Member State law. Businesses should: (i) review their existing compliance programmes, and ensure that those programmes are updated and expanded as necessary to comply with the Regulation; (ii) ensure that they have clear records of all of their data processing activities, and that such records are available to be provided to SAs upon request; and (iii) consider appointing a DPO.

New obligations of processors: The Regulation introduces ***direct compliance obligations for processors***. Under the Directive, processors generally are not subject to fines or other regulatory penalties. In an important change, under the Regulation processors may be liable to pay ***fines of up to €20 million, or 4% of annual worldwide turnover***, whichever is greater. The Regulation also requires detailed provisions in third-party processing contracts. This will have an impact on both controllers and processors, as they identify their processor agreements, review their commercial and legal positions for future agreements and renegotiate existing agreements.

Strict data breach notification rules: The Regulation will require businesses to notify the SA of data breaches ***within 72 hours***. If the breach has the potential for serious harm, individuals will have to be notified without undue delay. Businesses will need to develop and implement a data breach reporting and response plan (including designating specific roles and responsibilities, training employees, and preparing template notifications) enabling them to react promptly in the event of a data breach. The breach notification rule is likely to increase the risk profile for businesses, as their security breaches may get into public domain and attract attention of regulators and media.

Overview of the EU General Data Protection Regulation

Pseudonymisation: The Regulation introduces a concept of ***'pseudonymised data'*** (i.e., key-coded or enhanced data). Pseudonymous data will still be treated as personal data, but is likely to help organisations comply with the Regulation and reduce the risks of non-compliance. The 'key' necessary to identify individuals from the pseudonymised data must be kept separately and subject to technical and organisational measures to ensure non-attribution to an identified or identifiable person.

Binding Corporate Rules ("BCRs"): BCRs are binding data protection corporate policies and programmes that are used to lawfully transfer personal data globally within a group of companies. The Regulation formally recognises BCRs. They will still require SA approval, but the approval process should become ***less onerous than the current system***. BCRs are available to both ***controllers and processors***.

The 'right to be forgotten': Under the Regulation, individuals will have the ***right to request that businesses delete their personal data*** in certain circumstances (e.g., the data is no longer necessary for purposes for which it was collected). As a result, businesses will need to devote additional time and resources to ensuring that these requests are appropriately addressed. In particular, businesses should consider how they will give effect to the right to be forgotten, as deletion of personal data is not always straightforward.

The right to object to 'profiling': Under the Regulation, individuals will have the right to object to profiling on grounds relating to their particular situation. ***'Profiling'*** is defined broadly and includes most forms of online tracking and behavioural advertising, making it harder for businesses to use data for these activities. Businesses that regularly engage in profiling activities (e.g., in the advertising or social media context) will need to consider how to best implement appropriate consent mechanisms in order to continue these activities.

The right to Data Portability: Individuals will have ***the right to obtain a copy of their personal data from the controller in a commonly-used format and have it transferred to another controller.*** Consumer-based businesses (e.g., social media businesses, insurance companies, banks, telecommunication providers) should consider how they will give effect to these rights. Many new-to-market online businesses may welcome this new development as a way to improve competition in the sector while established providers will view it in less beneficial terms.

Contacts

Hunton & Williams

Bridget Treacy
+44 (0) 20 7220 5731
BTreacy@hunton.com

Wim Nauwelaerts
+32 (0)2 643 5814
WNauwelaerts@hunton.com

Dr. Jörg Hladjk
+32 (0)2 643 5828
JHladjk@hunton.com

Hunton & Williams LLP

Lisa J. Sotto
+1 (212) 309 1223
LSotto@hunton.com

Aaron Simpson
+1 (212) 309 1126
ASimpson@hunton.com

Centre for Information Policy Leadership

Bojana Bellamy
+44 (0) 20 7220 5703
BBellamy@hunton.com

privacy@hunton.com