KING & SPALDING

Client Alert

Data, Privacy & Security Practice Group

October 22, 2014

The General Data Protection Regulation
Update on the latest developments

Introduction

The European data protection directive is already one of the most stringent data protection laws in the world. Europe is set to have an even more rigorous data protection law with the introduction of the new General Data Protection Regulation (the "**Regulation**"). The most recent indication from the European Commission is that the Regulation is intended to be finalised in the first quarter of 2015.

Key Changes

There are number of key changes to the data protection regime under the Regulation:

1. **Territorial scope** – the Regulation will apply to all processing of personal data by a business operating in the European Union (**EU**) market, such as offering goods or services or monitoring of individuals, whether or not the business is physically based in the EU. It also applies to all data controllers and all data processors established in the EU, whether or not the processing takes place in the EU. All global businesses should, therefore, be aware of the new regime.

2. **"Data subject"** – the definition of a data subject under the current Directive is of a person who is identified or identifiable from the data by reference to an identification number or to one or more factors specific to the person's physical, physiological, mental, economic, cultural or social identity. This concept of indirectly identifying a person will be expanded under the Regulation to include methods of identifying an individual from his or her location data, genetic data or gender identity.

3. **"Pseudonymous" and "encrypted" data –** in addition to a definition of personal data are new definitions of: "pseudonymous data" meaning personal data that cannot be attributed to a specific person without using additional information, as long as the additional information is kept separately from the pseudonymous data and technical and organisational measures are used to ensure this data is not attributable to a specific person;

For more information, contact:

Pulina Whitaker
+44 207 551 7586
pwhitaker@kslaw.com

Clare Lynch
+44 207 551 7552
clynch@kslaw.com

King & Spalding
London
125 Old Broad Street
London EC2N 1AR
Tel: +44 20 7551 7500
Fax: +44 20 7551 7575

www.kslaw.com

and "encrypted data" meaning personal data which is rendered unintelligible by means of technological measures to any person who is not authorised to access it. Encryption of itself is, however, a form of processing of personal data.

4. **Consent** – under the Regulation consent will need to be explicit and freely given. The commonly used "opt out" method of obtaining consent is unlikely to be effective under the Regulation. Moreover, the data controller will need to prove consent was provided if challenged. Consent must be purpose-limited and will cease to be valid when the purpose is completed.

5. **Appointment of a Data Protection Officer** – for organisations with 250 or more employees, or where data processing is a core function, there will be a requirement for that organisation to appoint a Data Protection Officer. A group of companies can appoint a single Data Protection Officer.

6. **Data protection impact assessment** – data controllers will have to conduct data protection impact assessments if their processing operations present specific risks to the rights of the data subjects.

7. **Processor liabilities** – currently, data processors are not directly liable under the Directive. Data controllers are obliged to impose contractual obligations on their data processors but there is no direct liability under the Directive. This concept is replicated under the Regulation and, additionally, a data processor will be considered to be a data controller, with direct liability under the Regulation, if it processes personal data other than as instructed by the data controller.

8. **Data portability right** – this right under the Regulation gives individuals the right to obtain a copy of any personal data held about them by an organisation in a re-useable and electronic format. This is so that individuals are able to transfer their personal data from one service provider to another quickly and efficiently.

9. **Right to be forgotten** – this gives data subjects the explicit right to request that inaccurate data held about them be rectified and the right to request that any personal data held about them which is no longer necessary, or which they object to the data controller processing, is deleted. This right, which is not as explicit under the Directive, was the subject of a recent European Court of Justice ("**ECJ**") decision against Google.

10. **Fines for data protection breaches** – crucially the penalty for a breach of the Regulation will be significant. The data protection authority ("**DPA**") will be able to impose fines on an organisation which breaches the Regulation of the greater of: (a) 5% of its annual global turnover; or (b) EUR 100 million.

11. **Data breach notification requirements** – there will be a compulsory reporting obligation on a data controller to report a breach to its DPA without undue delay (in contrast to the previous proposed timeline of 24 hours). The breach must also be notified to the affected individuals where the breach is likely to affect adversely their data protection rights.

Areas of contention

Although the European Parliament has reached an agreement on certain aspects of the Regulation, there are some outstanding issues which are proving to be more difficult, such as the "one-stop shop" mechanism. In the current draft of the Regulation, organisations will only have to deal with the DPA in the jurisdiction of their "main establishment". This DPA would deal with any complaints raised by data subjects. Certain Member States, in particular Germany, believe that individuals who consider their data protection rights have been breached by an organisation should be able to seek recourse through their own DPAs, if different to that of the organisation.

Another issue which is proving to be contentious is the much publicised ECJ decision in *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González* on the right to be forgotten. In September 2014, the Article 29 Working Party, an independent and authoritative advisory body, met to discuss the Google decision. This follows their meeting earlier in July 2014 with representatives of Google, Microsoft and Yahoo! They concluded that it was necessary to have a coordinated and consistent approach to handling complaints against search engines and they said they would continue to monitor how search engines were complying with the decision. Guidelines for DPAs on how to process complaints and decisions made by other DPAs are currently being prepared and are intended to be finalised by November 2014.

Timing

Jean-Claude Juncker, the incoming President of the European Commission, has said that the Regulation should be finalised in the first quarter of 2015. Whilst this is a positive emphasis on finalizing the data protection reforms, given the lengthy European Parliamentary process and the matters which remain outstanding, it seems more likely that the Regulation will be finalised at some point in late 2015 or in 2016. The Regulation will be effective two years after it has been finalised and adopted by the European Parliament.

King & Spalding's Data, Privacy and Security Practice

King & Spalding is particularly well equipped to assist clients in the area of privacy and information security law. Our Data, Privacy & Security Practice regularly advises clients regarding the myriad statutory and regulatory requirements that businesses face when handling personal customer information and other sensitive information in the U.S. and globally. This often involves assisting clients in developing comprehensive privacy and data security programs, responding to data security breaches, complying with breach notification laws, avoiding potential litigation arising out of internal and external data security breaches, defending litigation, whether class actions brought by those affected by data breaches, third party suits, or government actions, and handling both state and federal government investigations and enforcement actions.

With more than 30 Data, Privacy & Security lawyers in offices across the United States, Europe and the Middle East, King & Spalding is able to provide substantive expertise and collaborative support to clients across a wide spectrum of industries and jurisdictions facing privacy based legal concerns. We apply a multidisciplinary approach to such issues, bringing together attorneys with backgrounds in corporate governance and transactions, healthcare, intellectual property rights, complex civil litigations, e-discovery / e-disclosure, government investigations, government advocacy, insurance recovery, and public policy.

* * *