ReedSmith

Global Regulatory Enforcement Alert

If you have questions or would like additional information on the material covered in this Alert, please contact one of the authors:

Cynthia O'Donoghue
Partner, London
+44 (0)20 3116 3494
codonoghue@reedsmith.com

Nick Tyler
Associate, London
+44 (0)20 3116 3695
ntyler@reedsmith.com

Katalina Chin
Associate, London
+44 (0)20 3116 2866
ckatalina@reedsmith.com

…or the Reed Smith lawyer with whom you regularly work.

European Commission's published draft General Data Protection Regulation: Detailed Analysis

Introduction

As reported in our January blog on the day of its release, the European Commission has now published a draft General Data Protection Regulation (the "Regulation") and has sent it to the European Parliament, along with a new draft Directive aimed at protecting personal data in relation to criminal investigations and judicial proceedings, including across borders.

Objective

With the Regulation, the Commission is attempting to achieve harmonisation of data protection regimes across Europe. Other stated objectives are to enhance individuals' rights and reduce administrative burdens and costly "red tape" for businesses. While the Regulation is certainly less draconian than the leaked draft with the introduction of two tiers of compliance obligations and reduced levels of sanctions, it may still be viewed with some trepidation. Ultimately, the Regulation presents a new set of burdensome challenges for many businesses and gives individuals more control over their data, in particular by addressing issues relating to children's use of the Internet. The Commission will seek to have European Parliamentary approval by the end of 2012, which if met, means a new data protection framework may be in force some time towards the end of 2014.

Scope

Article 3 of the Regulation limits its extra-territorial application to non-EU controllers processing personal data of EU-resident data subjects in relation to:

- the offering of goods or services to a data subject in the EU; or
- the monitoring of their behaviour.

Where any enterprise is outside the EU, it must appoint an EU representative unless it is headquartered in an EU-approved third country, employs less than 250 people or only occasionally offers goods or services to EU citizens.

Obligations on processors would increase by having to provide assistance to a controller in relation to data breaches or loss and the decommissioning of data at the end of the controller/processor relationship. In other respects, processors will have identical obligations imposed on them as controllers, specifically, for implementing appropriate security measures and being fully accountable to EU data protection regulators for their processing of personal data for which they would be directly liable.

There has been some relaxation of the scope of the Regulation, as compared with the previous leaked draft. For example, the documentation obligations of controllers and processors will not apply to any organisation employing less than 250 people, but only if their processing of personal data is "an activity ancillary to its main activities".

Definitions

While a number of definitions remain the same as in the existing Data Protection Directive 95/46/EC, additional definitions have been added, such as "personal data breach", which covers all types of security breaches, including when the data is in transit, being stored or otherwise processed.

The definition of health data has been broadened as well as changed to "data concerning health", which extends to "any information about the provision of health services to the individual." "Genetic data" and "biometric data" are separately defined reflecting the special treatment given to the processing of such data as presenting specific risks to individuals and thus requiring a privacy impact assessment and prior consultation with, and/or authorisation from the data protection

Client Alert 12-041
February 2012
reedsmith.com

authority under Articles 33 and 34 respectively.

Most notable is the change in the definition of "consent" in Article 4, which includes a requirement for consent to be "explicit" as well as "freely given, specific [and] informed". In addition, Article 7 sets out the following "conditions for consent", applicable to consent for processing sensitive personal data:

- the controller bears the burden of proving consent has been obtained, rather than it being assumed;
- consent for legitimising sensitive personal data processing cannot be wrapped up in a general consent to a set of contractual terms and conditions – it must be "distinguishable" from other matters;
- consent can be withdrawn (although such withdrawal would not de-legitimise processing based on previously given consent); and
- consent may be rendered invalid "where there is a significant imbalance" between the controller and data subject. In this last respect, the Regulation has stopped short of prescribing the employment relationship as one where there may be such an imbalance and so there may be circumstances where consent in the employment context can remain valid.

The lack of any specific protection for children in Directive 95/46/EC was a notable gap, particularly in the online and interactive world in which children fully participate. A new definition of "child" has been added, which is defined as anyone under the age of 18. The need for flexibility for teenage children (without which the Regulation would have proved unworkable) has been explicitly recognised and addressed by Article 8. This requires that the consent or authority of a parent or guardian is required for any child under the age of 13 specifically in relation to "the offering of information society services directly to a child". Controllers must make reasonable efforts to obtain verifiable consent, taking account of available technology. The provision does not affect the existing national contract law relating to children.

Data Protection Principles

The principles in the Regulation broadly correspond to the existing Directive 95/46/EC, although certain elements have been clarified in relation to:

- the transparency principle (to process fairly and in a transparent manner); and
- the purpose limitation principle has been relaxed in that it is no longer mandatory to get consent for processing for purposes which are incompatible with the purposes for which personal data was originally obtained. It will be possible for such purposes to be legitimised in other ways, including changing contractual terms and conditions.

Most notable is the new principle of accountability, which places full responsibility and liability upon controllers for each processing operation.

The accountability principle is meant to encapsulate good data protection practice and borrows certain principles from other data protection regimes, such as Canada, Australia and other Asia Pacific countries. As a result of this new principle, the existing notification requirements to data protection authorities fall away and instead are substituted by internal controls that document processing operations. Rather than having to comply with a myriad of different regulatory filing requirements, controllers will instead have to make available upon request to data protection authorities evidence demonstrating their data protection policies and procedures addressing their processing activities including time periods relating to retention and erasure, as well as 'privacy by design' and default mechanisms and privacy impact assessments.

Lawful Processing

The principle of lawful processing remains based on (i) consent; (ii) necessity for performance of a contract; (iii) legal requirement; (iv) vital interests; (v) public interest; and/or (vi) a controller's legitimate interests.

Legal requirements are explicitly limited to requirements within the EU, or of an EU Member State, and a controller's legitimate interests must override the fundamental rights of the individual, especially when the individual is a child.

The absolute bar on processing data which is subject to a legal requirement outside the EU aligns with prior decisions of the Article 29 Working Party, but may make it much more difficult for multinational companies to comply with legal requirements in other countries such as U.S. discovery rules, without resort to The Hague Evidence Convention. Where U.S. case law has required production of documents based on there not being a realistic prospect of prosecution, the new sanctions regime under the Regulation may change that view if an organisation is suddenly exposed to sanctions of up to 2% of its worldwide annual turnover for transferring data to the U.S. for use in litigation.

Where a controller is processing sensitive personal data, consent can only be relied upon subject to compliance with the conditions in Article 7 and, in the case of children, Article 8. In addition, either the law of the EU, or of a Member State, may provide that individuals' consent may not lift the general prohibition against processing sensitive personal data.

Rights of Individuals

In addition to the rights of access and rectification, the Regulation contains new rights for individuals, including the right to be forgotten, the right to data portability and to object to profiling.

The right to be forgotten is an extension of the existing rights of objection and rectification. It is intended to provide individuals with an opportunity to redress youthful indiscretions broadcast for posterity on social media sites and wipe the virtual slate clean. That objective has been emphasised in the Regulation by specific reference to "personal data which are made available by the data subject while he or she was a child".

The right to portability would allow an individual to transfer all of their data from one electronic provider to another, for instance where they wanted to move email accounts from one Internet based provider to another.

In relation to an individual's right to object to processing, the burden would be switched from the individual to the organisation to demonstrate that it has compelling legitimate grounds to continue processing the personal data.

Organisations would potentially be barred from profiling individuals based on automated processing that "produces legal effects" or "significantly affects" any individual by analysing and evaluating a person's performance at work, economic situation, location, health, personal preferences, reliability or behaviour unless done in the course of performing a contract, where consent (subject to conditions) has been obtained, or it is expressly authorised by law.
The right to object to direct marketing is a straightforward opt-out across the board. This will be of some comfort to many as the leaked draft had proposed the introduction of an opt-in standard for all commercial marketing. That said, the Regulation will not affect the separate provisions under the e-Privacy Directive and implementing rules governing unsolicited electronic marketing communications, which remain in force.

Data Protection Officer

Aligned closely with the introduction of the accountability principle is the requirement for both controllers and processors to designate a data protection officer (DPO). This will be imposed on:

- all public bodies,
- any private enterprise employing more than 250 people (a group of undertakings may appoint a single DPO), or
- any controller or processor whose core activities involve regular and systematic monitoring of data subjects.

The core duties of the DPO are set out in some detail and the independent status of the role, with legal protection given to the post-holder, is established as a non-negotiable requirement. While this measure may represent a not insignificant cost to many controllers, and for the first time to processors, it appears to be the price for the greater degree of self-regulation provided by the accountability principle for controllers and documentation requirements imposed on controllers and processors.

Privacy Impact Assessments and Prior Authorisation

Article 33 prescribes the following processing operations as presenting specific risks requiring controllers or processors to carry out a privacy impact assessment:

- systematic and extensive profiling of people's economic situation, location, health, personal preferences, reliability or behaviour;
- sensitive information used for the provision of health care, epidemiological research or health-related surveys that result in decisions or measures regarding individuals on a large scale;
- large scale video surveillance; and
- large scale filing systems on children, genetic or biometric data.

Where the privacy impact assessment concludes that the processing presents a high degree of risk then the data protection authority must be consulted and may require prior authorisation.

Data Breach Notification

The Regulation will introduce a general requirement on controllers to notify EU data protection authorities of data breaches (with the full support of their processors). The timescale for doing so will be within 24 hours of the breach, where feasible. Any notification later than that will need to be justified to the data protection authority. All notifications of breaches must be made to regulators – there will be no threshold of seriousness. Controllers will also have to notify individuals if the breach is likely to have an adverse effect on them unless the controller has demonstrated to the data protection authority that it has implemented appropriate security measures and, as such, breach notifications to data subjects are limited to more serious breaches.

Transfers to Third Countries

Transfers of data outside the European Union will still be permitted where adequate protection is established, including through the use of binding corporate rules (BCRs), standard data protection clauses or rulings of adequacy by the European Commission. The procedure for BCRs will be simplified and will automatically be accepted across all EU Member States upon authorisation.

Derogations to the transfer bar have been changed, with the most notable being that transfers may be made for the purposes of legitimate interests of the controller or processor so long as:

- they are not frequent or massive,

- the controller or processor has conducted a self-assessment of all relevant circumstances, and
- put in place appropriate safeguards.

Such assessment is consistent with the UK regulator's approach to 'self-assessment' of adequacy.

European Data Protection Board

A new supervisory body, the European Data Protection Board, will supersede the existing Article 29 Working Party and will work to ensure consistency of approach in the application of the Regulation, including the authorisation of BCRs.

Court Actions

At one point the European Commission was exploring the possibility of allowing individuals to bring class actions. However, the Regulation does not include such a provision, but does permit organisations aiming to protect individuals' rights to seek judicial remedies against controllers, processors or the relevant data protection authority.

Sanctions – the real cost of getting it wrong

The revised sanctions regime remains the key element that, with good reason, will capture everyone's attention. The Regulation sets out a harmonised and consistent approach to penalising controllers, their representatives and/or processors for infringements. Based on the principle that penalties "must be effective, proportionate and dissuasive" the Regulation provides three tiers of sanctions for intentional or negligent breaches of between 0.5%, 1% or 2% of an enterprise's annual worldwide turnover.

Breaches at the highest level of 2% include:

- processing personal data, and in particular sensitive personal data, without a legal basis or otherwise in breach of the relevant conditions;
- not designating a representative;
- failing to notify regulators and, if relevant, data subjects of a data breach; and
- not designating a data protection officer when required to do so.

The following factors will be taken into account in fixing the appropriate penalty: the nature, gravity and duration of the breach, the degree of responsibility of the controller or processor and their previous compliance record, the technical and organisational measures and procedures they have implemented, the degree of cooperation with the regulator shown and steps taken to remedy the breach.

The Regulation does introduce an element of leniency for first-time offenders who come within the category of an 'SME' (less than 250 employees and only ancillary processing of personal data) or a 'non-commercial individual', provided that their non-compliance is not intentional. In such cases the Regulation provides for a written warning, without sanction.

Conclusion

The Regulation contains a number of provisions that represent a softening of earlier draft proposals intended to address concerns expressed within the EU Commission and in the U.S. However, the inevitable compromises involved in meeting the late-January timeframe announced by D-G Justice, have resulted in two significant legislative fudges:

- The introduction of a new Section 5 – Article 21 – containing the basis of restrictions, or exemptions, to be made by EU or Member State law. The worrying aspect of this section is that it may lead to different provisions at national level and a continuing lack of harmonisation.
- Similarly, Article 82 identifies processing in the employment context as a specific data processing situation which may be subject to specific rules at national level. In our experience, recognising the need for alignment with different national labour laws across Europe will inevitably result in a different application of data protection rules across different Member States.

The European Commission's stated goal is to have parliamentary approval of the Regulation by the end of 2012. Despite some areas of uncertainty and the strong potential for continued disharmony, as well as the inevitable changes that will result from the legislative process, the Regulation provides enough detail in relation to the accountability principle and the increased self-regulatory regime for organisations to start preparing for implementation within the next three years.

About Reed Smith

Reed Smith is a global relationship law firm with more than 1,600 lawyers in 23 offices throughout the United States, Europe, Asia and the Middle East.