ReedSmith

European Commission's Proposed Change to the EU Data Protection Laws: Detailed Analysis

Author: Cynthia O'Donoghue, Partner, London
Author: Nick Tyler, Associate, London
Author: Katalina Chin, Associate, London

Publication Date: December 13, 2011

Introduction

In advance of formal publication, the European Commission sent the proposed Data Protection Framework for the EU for inter-service consultation with the Directorates-General, which consists of a Data Protection Regulation and a new Police and Criminal Justice Data Protection Directive. Following this period of consultation, the European Commission's final draft will be submitted to the European Parliament, with the timing estimated during the latter part of January 2012. These documents were first leaked to the press, and highlighted in our recent blog. Originals can be obtained at Statewatch.

Objective

The European Commission has sought to fulfil its long-stated ambitions of harmonising the data protection regime across Europe, and of enhancing individual's rights. While one of the stated objectives is also "cutting red tape for businesses", it is difficult to see how this objective has been met in the draft documents, given the increased burdens on industry. Another stated objective of the Commission was to give individuals more control over their data, to address issues related to children's use of the Internet. The Commission will seek to have European Parliamentary approval of the Framework by the end of 2012, which, if met, means a new Data Protection Framework may be in force sometime in 2013.

Scope

If there was ever any doubt as to whether European data protection law applied outside the EU, then this draft regulation should remove it. Article 2 explicitly extends the scope of the regulation

to any controller, established inside or outside of the EU, who processes personal data of EU citizens. Where an organisation is outside the EU, it must appoint an EU representative.

More surprising is that the Regulation will apply to individual persons who make the "personal data of other natural persons [sic] accessible to an indefinite number of individuals"; in other words, the regulation applies to individuals who post others' personal data on the Internet.

Obligations on processors would increase by having to provide assistance to a controller for data breaches or loss, and in relation to 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.

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 consent of health data has been broadened as well as changed to "data concerning health", which extends to eligibility for health services, and includes separate definitions for "genetic data" and "biometric data". Most notable is the change in the definition of "consent", which includes a requirement for consent to be "explicit".

A new definition of "child" has been added, which is defined as anyone under the age of 18, and if it remains in its current form may conflict with some organisations' practices in allowing children over 13 access and membership to websites without first seeking parental consent, or when providing them with targeted marketing, since that will also require parental consent for children under 18.

Data Protection Principles

The principles in the draft Regulation broadly correspond to the existing Data Protection Directive, although certain elements have been clarified or extended in relation to the transparency principle (processes fairly and in a transparent manner), the data minimisation principle (limited to the minimum data necessary and only processed if it's not possible to do so

in a de-identified manner), and a new purpose 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 falls away and instead is substituted by internal controls that document processing operations. Rather than having to comply with myriad and 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 assessment.

Lawful Processing

Lawful processing remains based on (i) consent, (ii) necessity for performance of a contract, (iii) legal requirement, (iv) vital interests, (v) public interest and (vi) a controller's legitimate interests.

Legal requirements are now explicitly limited to requirements within the EU or of a 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 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 multi-national companies to comply with legal requirements in other countries, such as the 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 proposed Regulation may change that view if an organisation is suddenly exposed to sanctions of up to 5 percent of its worldwide annual turnover for transferring data to the United States for use in litigation.

Controllers will now have to prove that they have been provided with consent, and consent may not be relied upon if there is a "significant imbalance in the form of dependence between the position of the data subject and the controller", which would make it nigh on impossible, for example, for employers to obtain employees' consent. In addition, where a controller is

processing sensitive personal data, there may be certain instances where consent cannot be validly obtained because either the law of the EU or of a Member State prohibits it.

Controllers would only be able to process personal data for commercial direct marketing purposes based on explicit consent, and opt-outs would only apply to marketing for non-commercial purposes "recognised as being in the public interest", presumably covering marketing for political or charitable causes.

Rights of the Individuals

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

The right to be forgotten is an extension of the previous right of objection and erasure. 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.

The right to portability would allow individuals 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 ground to continue processing the personal data.

rganisations would potentially be barred from profiling individuals based on automatic processing that seeks to predict a person's performance to work, creditworthiness, economic situation, location, health, personal preferences, reliability or behaviour; unless done so in the course of performing a contract, consent has been obtained or is expressly authorised under law.

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. This will be imposed on all public bodies and any private enterprise employing more than 250 people. The core duties of the data protection officer 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, it appears to be the price for a greater degree of self-regulation.

Data Breach Notification

As widely predicted, the regulation will introduce a general requirement on controllers (with the full support of their processors) to notify EU data protection authority of data breaches within 24 hours. Controllers may also have to notify individuals if the breach is likely to have adversely affected them unless the controller has demonstrated to the authority that it has implemented appropriate security measures.

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, standard data protection clauses or rulings of adequacy by the European Commission. The procedure for BCRs is to be simplified and will be automatically 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 legitimate interest of the controller or process so long as they are not frequent, massive, or structured, and adequate safeguards are in place.

European Data Protection Board

A new supervisory body, the European Data Protection Board, will supersede the existing Article 29 Working Party and ensure consistency of approach, enforcement in relation to all aspects of the Data Protection Framework, including authorisation of BCRs, and the enforcement mechanisms.

Court Actions

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

Sanctions - the real cost of getting it wrong

Easily the most headline-grabbing aspect of the draft Regulation is the new sanctions regime, which 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 draft Regulation provides three tiers of sanctions for intentional or negligent breaches of between 1 percent, 3 percent or 5 percent of an enterprise of annual worldwide turnover. Breaches at the highest level of 5 percent include:

- Processing personal data, and in particular sensitive personal data, without a legal basis or otherwise in breach of the relevant restrictions
- Not designating a representative
- Failing to notify regulators and, if relevant, data subjects of personal data breach
- 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; and the degree of cooperation with the regulator shown and steps taken to remedy the breach.

Conclusion

While this is only a draft of the new Data Protection Framework, and it is unlikely to be either submitted or enacted by the European Parliament in its current form, the draft Framework does contain quite a few provisions that will most likely be enacted. What remains to be seen is whether the sanctions, which will elevate the penalties for non-compliance to a level similar to anti-trust, will remain.

With so many substantive changes, it is also hard to know whether the changes will have a knock-on effect on the presently lawful bases for transfers of personal data outside the EU, such as that the existing EU Standard Contractual Clauses, the U.S. Safe Harbor Framework, to the list countries approved as by the Commission as providing adequate protection, or even whether organisations with BCRs will have to amend them and seek re-authorisation.

The European Commission's stated goal is to have Parliamentary approval by the end of 2012. Despite the changes that may come as a result of the legislative process, the draft Regulation provides enough detail in relation to the principle of accountability and the increased self-regulatory regime for organisations to start preparing.

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.