EUGENE F COLLINS

Intellectual Property / Information Technology Group

New EU Data Protection Regulation… It's Getting Closer!

Date: 25 January 2014

New EU Data Protection regulation… it's getting closer!

Recent media publicity regarding mainstream data security breaches such as that involving Loyaltybuild and SuperValu, has brought the issue of data protection sharply into focus. Major changes in the law at an EU level have been signalled and in order to plan and prepare for compliance in the future, businesses should act now to consider how these changes will impact their organisations and method of operating.

Proposed Reform of Data Protection Legislation

In 2012, the European Commission signalled a major reform of the EU Legal Framework on the Protection of Personal Data. The European Commission has proposed that the reform of the EU Legal Framework on the Protection of Personal Data will be achieved through the introduction of a new Data Protection Regulation ("the Regulation"). The Regulation will apply uniformly throughout individual EU Member States without the requirement for any national implementing legislation to give it legal effect. This brings a much-needed harmonisation of data protection law across the Single European market would be achieved. Organisations should note that change is coming and take steps in the interim period to plan how they will comply with the new regime.

Background

The current EU Data Protection Directive, 95/46/EC ("the Directive"), dates back to 1995 and is now viewed as being outdated, particularly given developments in e-commerce, big data and large-scale information processing. In addition, the requirement for individual EU Member States to implement the Directive by way of national legislation has led to a variation in standards and requirements regarding data protection across the EU, and this is viewed as being incompatible with the desire to have a single set of standards applicable to the Single European market.

Key Proposed Changes

Whilst the precise wording of the Regulation is being discussed and debated, it is clear that there will be a number of significant changes from the current EU regime, including:

1 Increased Fines

Current indications are that fines of up to €100 million or 5% of annual worldwide turnover may be imposed for breaches.

2 Wider Territorial Scope

The Regulation will apply to organisations outside the EU whenever they process personal data in connection with the provision of services to, or monitoring of, individuals located in the EU.

3 Freely Given Consent

A service cannot be made conditional on a user giving consent to the processing of personal data that is not necessary for the service.

4 Changes to Sensitive Data

The definition has been expanded to cover "gender identity" and has also expanded the legal grounds for processing such special categories of data to include performance or execution of a contract and processing necessary for archiving purposes.

5 Security Monitoring/Disclosure Third Party Authorities

Additional provisions are included to provide a data subject with the right to know if his/her personal data has been disclosed to a public authority at the authority's request. In addition, the transfer of personal data required by a third country Court decision or by an administrative authority is prohibited if such a transfer would not be compliant with a mutual legal assistance treaty or international agreement. There are further changes proposed to the current exemptions in place for frequent or large-scale data transfer and use of traffic and location data by public authorities for safeguarding national security and law enforcement activities.

6 Right to be Forgotten

The much-talked about "right to be forgotten" is now being referred to as a "right to erasure" and there have been some additional clarifications where a particular type of storage technology does not allow for erasure, then the data subject has a right to have the data "restricted" as opposed to erased.

7 Data Breaches

It is likely that where a data security breach occurs there will be mandatory notification requirements to data subjects and other relevant authorities as opposed to relying on the current voluntary schemes in place under the current regime.

8 Data Protection Officer

Certain organisations will be required to appoint a dedicated Data Protection Officer. The threshold for appointing a Data Protection Officer will be the number of people whose data is processed in the organisation, being 5,000 data subjects in any consecutive 12-month period. Previously, it was thought that the number of personnel within an organisation would be the trigger point for appointment of a dedicated Data Protection Officer. The Data Protection Officer must be appointed for a minimum term and must also have certain minimum qualifications.

9 Supervisory Authorities

The concept of a one-stop shop which was previously discussed whereby organisations would have a single supervisory/regulatory authority overseeing their data processing activities across all EU Member States is now likely to be replaced by a "lead authority" which would be required to consult with all other competent authorities. It is likely there will be significant further discussion on this point in order to clarify specific supervisory requirements.

Timing?

It was previously anticipated that the proposed data protection reforms could be finalised before the European Parliamentary elections taking place in May of this year. However, it now seems likely that the Regulation will not be passed until 2015, and there will be a further period of time before the Regulation comes into force.

For further information on this topic please contact: David Hackett, Partner, Intellectual Property/ Information Technology Group, E: dhackett@efc.ie