LK SHIELDS
YOUR LEGAL COUNSEL

TECHNOLOGY

Privacy by Design and by Default

by

Privacy by Design and by Default

18th September 2017 | by

The privacy concepts of "Privacy by Design" and "Privacy by Default" will for the first time be explicitly recognised in Irish law under Article 25 of the new General Data Protection Regulation (GDPR), when it comes into force across EU Member States in May 2018. These concepts require privacy considerations to be factored into a product, service or project at the very outset of its development. As such, organisations will need to consider data privacy at the initial concept and design stage of a product, service or project and throughout its life cycle.

The GDPR will be the first time that these concepts will be codified into Irish law. The current EU Data Protection Directive (Directive 95/46EC) and the Irish data protection legislation, the Data Protection Acts 1988 and 2003 (as amended), do not recognise the concepts of privacy by design and by default. While these concepts are not recognised under Irish law, they are not new, but have to date largely been considered best practice and will be familiar to many readers already.

How to approach privacy by design

In practical terms, privacy by design should be considered as early as possible in the product/service lifestyle, often this will be at the same time that a data protection impact assessment (DPIA) is conducted by the organisation, enabling it to identify and assess the data privacy risks and challenges associated with the product, service or project, and how these can be best managed.

The types of items that will be considered in a DPIA are: types and quantities of data collected, data flows and disclosures, data minimisation technologies and security. Following the DPIA, technical and other measures should be implemented so as to minimise any data privacy issues identified.

The benefit of building privacy by design at an early stage into your products, services and projects, is that this will assist in alleviating data protection concerns that might otherwise arise at a later stage.

How to approach privacy by default

The GDPR requires that user settings should have the most privacy friendly setting as the default setting. Under the GDPR, organisations are required to implement appropriate measures both on an organisational and technical level so that, by default, only personal data which are necessary for each specific purpose of the processing are processed. For this reason, there is a greater emphasis on employing data minimisation techniques such as pseudonymisation so that only the minimum amount of data required is collected and processed. As such, organisations should assess the amount and extent of personal data collected and processed, and also how long it is stored and who can access it.

Similarly to privacy by design, privacy by default should be integrated into your projects, services and products from the very outset. In this regard, it is important to carry out a DPIA in order to measure their compliance with privacy by default.

Obligations on public authorities

The GDPR is an EU Regulation and generally Regulations do not require further national implementing legislation, as they are intended to harmonise the law across the EU. The GDPR is different in this regard. The GDPR gives Member States a margin of discretion in certain areas that it covers and therefore will not fully harmonise EU data protection laws. For this reason, a new Data Protection Bill 2017 is currently being drafted in Ireland to provide for certain derogations from the GDPR and to also ensure that Ireland has fully implemented the provisions of the GDPR. So far, a General Scheme has been published which sets out various provisions that may be included in the new Data Protection Bill 2017.

The General Scheme specifically mentions that public authorities and other entities charged with preventing investigating, detecting or prosecuting criminal offences (e.g. An Garda Síochána) or imposing criminal penalties, including safeguarding against and preventing threats to public security will be required to abide by the principles of privacy by design and by default.

Factors to take into account in the implementation of privacy by design and by default

The GDPR has set out a number of factors for organisations to take into account when implementing privacy by design and by default:

- the state of the art and technological development.
- the cost of implementing privacy by design and by default.
- the nature of the data concerned.
- the scope, context and purposes of processing such data.
- the risks to an individual's privacy and the likelihood (and severity) of such arising from the processing of their personal data.

The factors to be taken into account in each case will vary and the assessment of such will depend on, among other things, the nature of the product, project or service for example.

Certification

The GDPR also notes that compliance with the concepts of privacy by design and by default can be demonstrated by following an approved certification mechanism. To date, we are not aware of any approved certifications to demonstrate GDPR compliance, but this may change. In the meantime, it is important to document the steps taken to embed privacy by design and by default into your products, processes, projects and services for example.

We are closely monitoring the developments of the General Scheme and the implementation of the GDPR in Ireland and will keep you updated. If you would like information as to how the GDPR will affect your business, please contact Aideen Burke.

About the Author