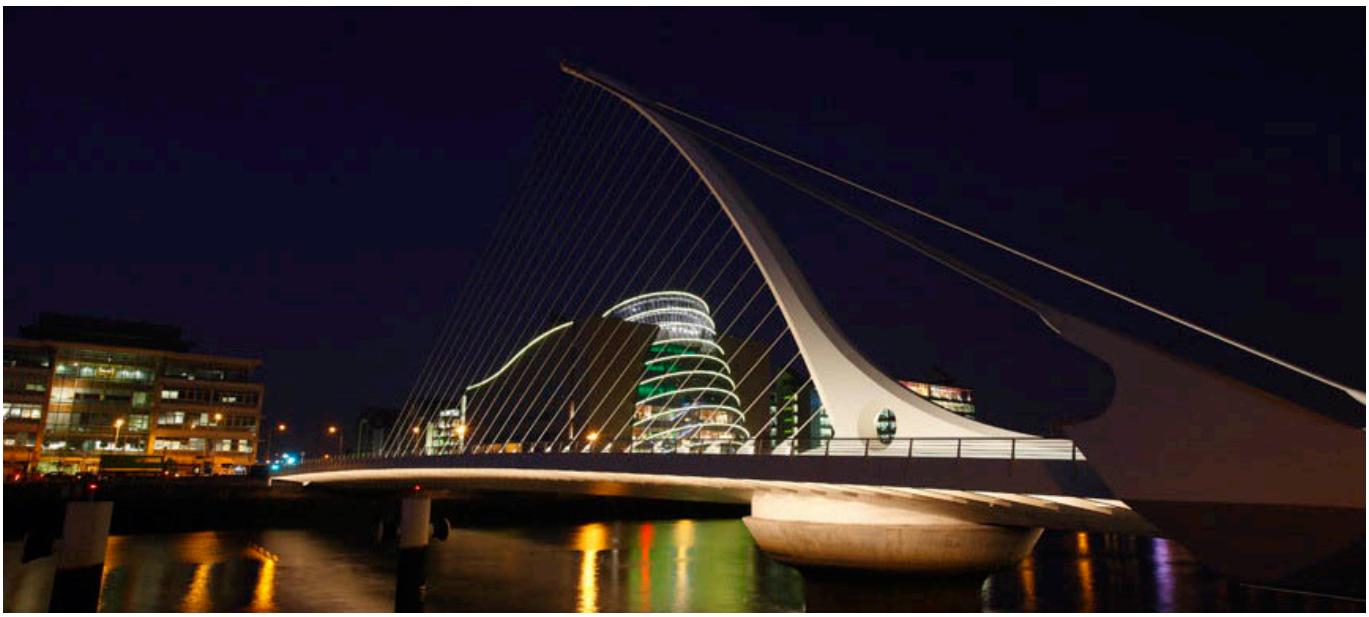
GDPR in Context: Overview of GDPR

Background

The General Data Protection Regulation (the "**GDPR**") will come into effect on 25 May 2018. The GDPR will be directly effective in each EU member state, with the aim that the same rules will be applied uniformly within the EU. This marks a shift in the approach to data protection at a European level, which until 25 May 2018 will rely on national implementing legislation in each EU member state.[1]

The period between now and 25 May 2018 is therefore the de facto transition period, during which organisations will need to assess their current approach to data protection, to undertake a gap analysis between that current approach and the requirements under the GDPR, and to implement any changes and improvements which are required to achieve demonstrable compliance with those GDPR requirements.



Overview of GDPR

The GDPR puts personal data protection front and centre as a fundamental right of the individual, and introduces the concept of data privacy "*by design and by default*", which is in effect a recasting of the data protection principles and security obligations under the current EU Data Protection Directive (which has been implemented into Irish law through the Data Protection Acts 1988 and 2003 (the "**DPA**")). Allied to the by design and by default theme, is an emphasis on transparency and accountability as fundamental GDPR concepts, necessitating that compliance with the relevant requirements be demonstrable.

Another important feature of the GDPR is the extension of scope of EU data protection rules, with the GDPR applying not only to controllers established in the EU, but also to non-EU controllers and processors if the processing relates to offering goods and services to individuals in the EU or monitoring the behaviour of individuals insofar as the behaviour takes place in the EU.

The GDPR introduces the concept of a 'one stop shop' for supervision (subject to co-operation between data protection authorities), which will require multinational organisations in particular to establish which EU supervisory authority should be their lead authority.

The design element of the GDPR requires controllers, having regard to the state of the art and cost, to implement appropriate technical and organisation measures and procedures ensuring compliance with the GDPR. Controllers will also be expected to implement mechanisms which, by default, ensure that data can only be processed in accordance with rules which reflect the data protection principles in the GDPR.

As a corollary of the re-focused approach, and the emphasis on transparency and accountability, there is and will be additional focus on processing arrangements, including a strengthening of security obligations imposed directly on processors. However, there is equally an increased focus on the responsibility of controllers for choosing processors providing sufficient guarantees to implement appropriate technical and organisational measures and procedures in such a way that the GDPR requirements are met and the rights of data subjects are protected, and for ensuring ongoing compliance by those processors.

In addition, the GDPR imposes new requirements relating to the analysis and documenting of data processing activities as part of efforts to ensure controllers are accountable for and can demonstrate compliance with the GDPR. Both controllers and processors will have to keep more detailed records of their data processing activities, and there will be a requirement for privacy impact assessments ("**PIAs**") if the processing involves an increased level of risk, which may require pre-processing consultation with the relevant supervisory authority.

---

[1]There will be national implementing legislation with regard to certain elements, in particular the sanctions regime. However, the general principles which govern the processing of personal data by both controllers and processors will apply automatically from 25 May 2018.

Overview of GDPR

Furthermore, breach notification to supervisory authorities will become mandatory following implementation of the GDPR, with notification required without undue delay and, where feasible, within 72 hours of the controller becoming aware of same. Notification to data subjects, without undue delay, will also be necessary where the breach is likely to result in a high level of risk to the data subjects.

Restrictions on transfers abroad will continue to apply, with some of the grounds upon which transfers are permitted drafted more narrowly than is currently the case under the DPA.

Under the GDPR, the appointment of a data protection officer ("**DPO**") will be required where:

(i) the processing is carried out by a public authority or body (with the exception of the courts);

(ii) where the core activities of the organisation consist of:

(a) processing operations which require regular or systematic monitoring of data subjects on a large scale; or

(b) processing large amounts of special categories of personal data.

The GDPR also extends the number and scope of individual rights, making consent more restrictive as a basis for legitimate and lawful processing of an individual's personal data, requiring greater transparency in relation to the justification for the processing, and giving greater rights to object to processing, and in relation to data portability and the 'right to be forgotten'.

Finally, the GDPR will introduce much tougher sanctions for breach, modelled on existing sanctions for breach of competition law, with maximum penalties for intentional or negligent breaches of up to EUR 20 million or 4% of an undertaking's annual worldwide turnover.

Next steps

The significant strengthening of data protection rules which is inherent in the GDPR, and in particular the sanctions under the GDPR, emphasise the need to ensure that each organisation has full insight into the data flows concerning customer data and other personal data which it controls, and that it puts appropriate notifications, processing agreements, transfer arrangements and security arrangements in place.

The starting point for any GDPR compliance project is therefore an understanding of the "*what, why, how and where*" of current personal data processing by each organisation, and where appropriate by department or business line within the organisation. What personal data is held and used, why the organisation needs and uses it (which may not necessarily be the same thing), how the personal data is processed and shared, where it is stored and from where it is accessed – all of these are important questions to be answered before it will be possible to undertake the necessary gap analysis.

Contacts

Anne-Marie Bohan
PARTNER
D +353 1 232 2212
E anne-marie.bohan@matheson.com

Deirdre Kilroy
PARTNER
D +353 1 232 2231
E deirdre.kilroy@matheson.com

Chris Bollard
PARTNER
D +353 1 232 2273
E chris.bollard@matheson.com

Carina Lawlor
PARTNER
D +353 1 232 2260
E carina.lawlor@matheson.com

Christine Woods
ASSOCIATE
D +353 1 232 2147
E christine.woods@matheson.com

12.10.17