Deloitte.

GDPR Compliance
The clock is ticking

The European Commission first proposed the text of the EU General Data Protection Regulation (GDPR) back in 2012. Fast forward to four years of negotiation later, we now have a finalised text, published in the Official Journal of the EU on 4 May 2016 and entered into force on the 25 May 2016. This Regulation (2016/679) along with a new Data Protection Directive (applicable to the law enforcement sector) will replace the current Data Protection Directive 95/46/EC, and is directly applicable in all Member States.

Why?

Harmonisation across Member States paves the way to a more consistent and uniform approach which will be welcomed by multinational companies. Modernisation of the current framework sets the scene for greater privacy for individuals as well as addressing the privacy challenges of a data rich generation and the administrative and costly burden of multiple data protection authorities (DPAs) will be reduced.

However, with reform, inevitably comes uncertainty. Companies have until 25 May 2018 to ensure they are compliant and while the GDPR takes away a lot of the existing complexity in this area, the regime is certainly a stricter one with action required by companies to ensure operational compliance by the deadline.

How?

The GDPR brings some key changes in the following areas:

Applicability and One Stop Shop

The territorial scope under the GDPR is now broader and is applicable to data processors and now also data controllers who are situated outside of the EU but who offer goods and services within the EU. The one-stop-shop idea is also quite attractive to companies that are situated in multiple EU jurisdictions. Instead of dealing with DPAs in each jurisdiction, the GDPR allows for a 'lead' DPA who will be the DPA in the main establishment of the company. This DPA will supervise all cross border processing activities and will work closely with other DPAs to involve them in the decision making process when necessary. DPAs in other relevant jurisdictions can handle cases involving national citizens but the 'lead' DPA has the right to take over and handle the case.

Data Security and Breach Notification

Any data breach or potential data breach must be reported to the DPA within 72 hours. The only exception is if the breach is unlikely to be a high risk to the privacy of individuals. If the breach is likely to be high risk, then affected individuals must also be notified without delay.

Mandatory DPO

There is a mandatory obligation to appoint a Data Protection Officer (DPO) for public bodies as well as controllers and processors whose core activities involve regular and systematic monitoring of data subjects on a large scale basis and/or large scale processing of special categories of personal data. The DPO can be a full-time employee or hired on a consultancy basis but they must have expert knowledge of data protection law and practices, must have adequate resources to fulfil their role, significant independence in the performance of their role and a direct reporting line to the highest level of management.

Accountability and Governance

The GDPR strengthens the importance of accountability which requires adherence with all principles and the ability to

demonstrate compliance. In order to do this, there is an expectation to put in place comprehensive and proportionate governance measures. Privacy Impact Assessments (PIAs) must be carried out prior to any processing of personal data where there is a high privacy risk and it is mandatory, at the outset of every new design (system, process, service etc.), to ensure data protection considerations are taken into account (Privacy by Design). In addition, Privacy by Default must be the norm where there is a choice in sharing personal data and the norm must be the most privacy friendly one.

Duties and Responsibilities of Controllers and Processors
There is an increased obligation on processors to directly comply with data protection legislation. Whereas in the past, the burden lay predominantly at the controller's feet, processors will now be accountable and responsible under the law. Controllers must ensure they have detailed contract terms with processors and maintain records of all processing activities and may be required to make this information available to the DPA upon request. In addition, the DPA can go to the processor directly with any requests.

Consent
While consent has always existed in terms of implicit and 'opt-out' consent, under the GDPR, consent must be backed up by a statement or a clear affirmative action and must be unambiguous. Silence, pre-ticked boxes or inactivity will no longer infer consent.

Data Subject Rights
The rights of data subjects under the GDPR are now strengthened and broadened, giving more control to individuals. The right to data portability allows an individual to transport personal data from one organisation/service provider to the other, facilitated by the organisation in a structured, commonly used and machine-readable format. The right to be forgotten (or erasure) enforces an individual's right to erasure of his/her personal data and to prevent processing once it is clear that the processing is unlawful.

International Data Transfers
Similar to the Directive, the GDPR allows the transfer of personal data outside of the EU to countries whose legal regime is deemed to provide an adequate level of protection by the European Commission. Where there is no adequacy, transfers will still be allowed outside of the EU under certain circumstances, such as through the use of standard contractual clauses or binding corporate rules (BCRs).

Administration and Fines
The administrative burden under the GDPR has eased somewhat with the abolishment of the requirement to register with DPAs, however, the most impactful change under the GDPR is the increased scope in terms of administrative fines that can be incurred for non-compliance or violation:

- The lessor threshold is a potential fine of €10 million or 2% of total worldwide annual turnover (whichever is greater) for serious breaches; and
- The higher threshold is a potential fine of €20 million or 4% of total worldwide annual turnover (whichever is greater) for very serious breaches.

Codes of Conduct and Certifications
Codes of conduct and certifications along with privacy seals are introduced and encouraged in order to prove adherence with the GDPR. The GDPR encourages the submission of codes of conducts to DPAs for consideration in order to grow this mechanism in the coming years.

European Data Protection Board
The Article 29 Working Party is to be replaced by an independent European Data Protection Board (EDPB) and will be made up of a Supervisor along with the representatives of all national DPAs. The EDPB will issue guidance, opinions and ensure a consistent application of the GDPR across all DPAs.

The clock may be ticking but there is still time. We are in a transition period where next steps are key. Looking at how the GDPR impacts your organisation in terms of operational, technical and legal aspects is important now as well as taking action to fill any gaps that exist.

For more information on the GDPR or for any data protection and privacy questions including tailored assessments, please contact the Deloitte Ireland Privacy Team.

Contacts

For more information please contact:

Nicola Flannery
Manager | Risk Advisory
Tel/Mob: +353 87 1703 072
Email: niflannery@deloitte.ie

Kelvin Garrahan
Senior Manager | Cyber Risk Services
Tel/Mob: +353 87 297 5396
Email: kgarrahan@deloitte.ie

Donal Murray
Director | Risk Advisory
Tel/Mob: +353 87 099 8884
Email: donmurray@deloitte.ie

Sean Smith
Partner | Risk Advisory
Tel/Mob: +353 86 852 7597
Email: seansmith1@deloitte.ie

Dublin
Deloitte
Deloitte & Touche House
Earlsfort Terrace
Dublin 2
T: +353 1 417 2200
F: +353 1 417 2300

Cork
Deloitte
No.6 Lapp's Quay
Cork
T: +353 21 490 7000
F: +353 21 490 7001

Limerick
Deloitte
Deloitte & Touche House
Charlotte Quay
Limerick
T: +353 61 435500
F: +353 61 418310

Galway
Deloitte
Galway Financial Services Centre
Moneenageisha Road
Galway
T: +353 91 706000
F: +353 91 706099

Belfast
Deloitte N.I. Limited
19 Bedford Street
Belfast BT2 7EJ
Northern Ireland
T: +44 (0)28 9032 2861
F: +44 (0)28 9023 4786

deloitte.ie

Deloitte.