INSTITUTE OF DIRECTORS IN IRELAND

McCann FitzGerald

IoD & McCann FitzGerald GDPR – A Director's Guide to GDPR Implementation

1st February 2018

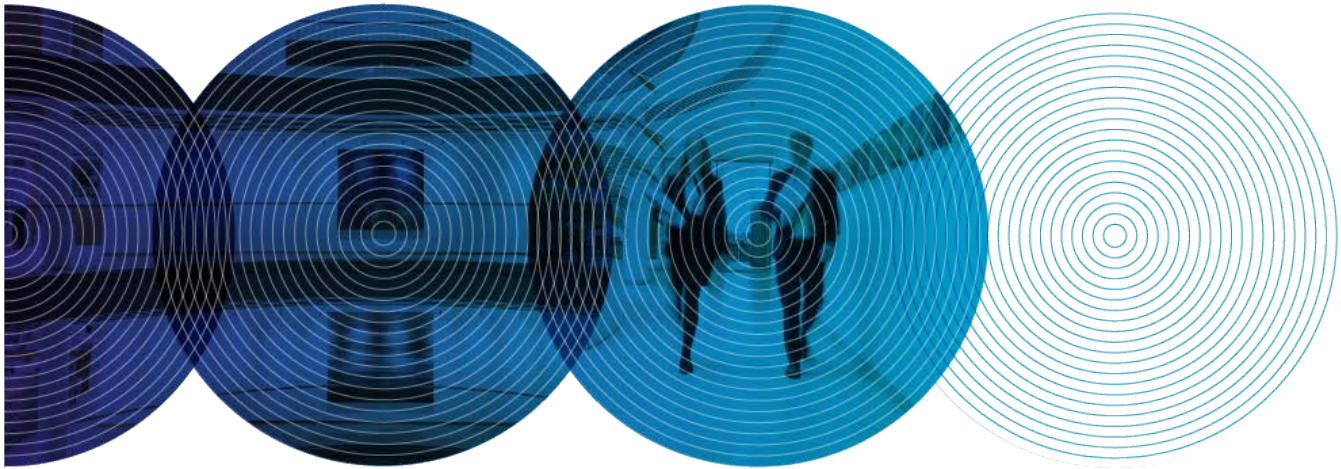
@IoDIreland @McCannFitz #IoDEvents

Institute of Directors and McCann FitzGerald

Countdown to GDPR

Paul Lavery, Partner, Head of Technology & Innovation

Thursday, 1 February 2018



McCann FitzGerald

INSTITUTE OF DIRECTORS IN IRELAND

Introduction and Today's Topics

- General Data Protection Regulation – Countdown
- Recent Survey on GDPR Readiness – Main findings
- Areas of most concern to Irish Business

Countdown to GDPR

- General Data Protection Regulation - Replaces existing law in all member states on 25 May 2018
- Designed to result in single, uniform set of data protection rules applying across the EU
- Irish Data Protection Bill – General Scheme for Bill published on 12 May 2017 - designed to be main Irish legislative instrument to give effect to, or provide for exemptions from, certain provisions of the GDPR
- Bill expected ***this week***

Recent Survey on GDPR Readiness

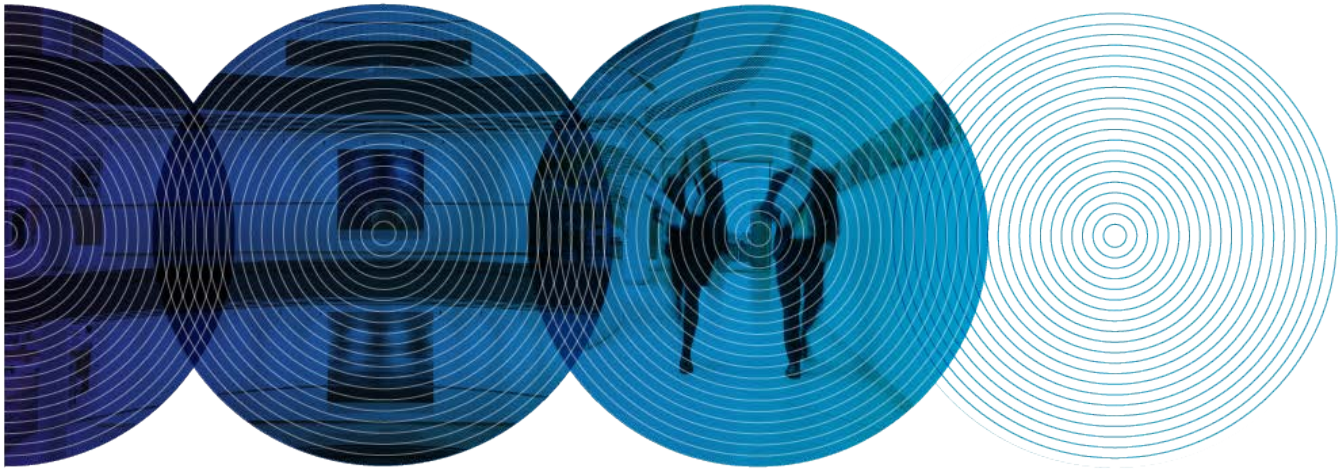
- The more organisations review their operations, the more they realise that there are key challenges
- 95% of organisations think that meeting GDPR compliance requirements will be challenging
- Areas of key concern:
  - outsourcing implications including international transfers within and outside EEA
  - data protection/privacy notices and methods of consent
  - record of processing operations/data inventory
  - the role of the Data Protection Officer

Institute of Directors and McCann FitzGerald

GDPR - Areas of Concern for Irish Business

Paul Lavery, Partner, Head of Technology & Innovation

Thursday, 1 February 2018



McCann FitzGerald

INSTITUTE OF DIRECTORS IN IRELAND

Outsourcing/Use of Data Processors

- Article 28
- Will the outsource service provider have access to and process personal data on your behalf?
- Use only processors providing sufficient security guarantees
- Processor not entitled to engage sub-processor without controller consent

Outsourcing/Use of Data Processors *cont'd*

- Requirement to have contract with processor which includes various provisions (more detailed than required under existing law), including:
  - processing in accordance with instructions
  - security measures;
  - confidentiality obligations
  - audits and inspections
  - notification of data security incidents
  - return or deletion of data on expiry of processing services

Outsourcing/Use of Data Processors *cont'd*

- Level of assurance required – risk based analysis

Transfers Abroad

- Prohibition on Transfer of Personal Data outside European Economic Area (EU, Iceland, Norway and Liechtenstein) unless recipient country ensures adequate protection
- Andorra, Argentina, Canada, Faroe Islands, Guernsey, Isle of Man, Israel, Jersey, New Zealand, Switzerland and Uruguay found to have adequate protection

Transfers Abroad *cont'd*

- Prohibition will not apply, amongst other things, if:
  - data subject consent
  - transfer necessary for purpose of obtaining legal advice or for legal proceedings
  - data transfer agreement, using standard contractual clauses in the form approved by the European Commission
  - binding corporate rules
  - privacy shield (if transfer is to United States)
- Brexit Implications

Data Protection Notice

- Form - Article 12
  - concise, transparent, intelligible, easily accessible, using clear and plain language
  - in writing, by other means (including electronic)
  - orally where requested by data subject (provided identity of data controller proven by other means)
  - content - Articles 5(1)(a), 13 and 14
    - identity/contact details of controller/DPO
    - purposes of processing/legal basis for processing
    - recipients of personal data

Data Protection Notices *cont'd*

- Legitimate interests/right to withdraw consent (where relevant)
- Transfers abroad – measures taken
- Data subject rights (access, portability, rectification, objection, erasure)
- Right to lodge a complaint with the supervisory authority
- Whether provision of data a statutory or contractual requirement – consequences of not providing data
- Existence of automated decision making (including profiling)

Methods of Obtaining Consent

- Article 6(1) – legal basis for processing
- Freely given, specific, informed and unambiguous
- Should not be bundled with other consents
- Intelligible, easily accessible, clear and plain language
- Ban on pre-ticked boxes
- Right to withdraw at any time
- Provision of a service must not be made conditional on consent to non-essential forms of processing

Alternatives to Consent

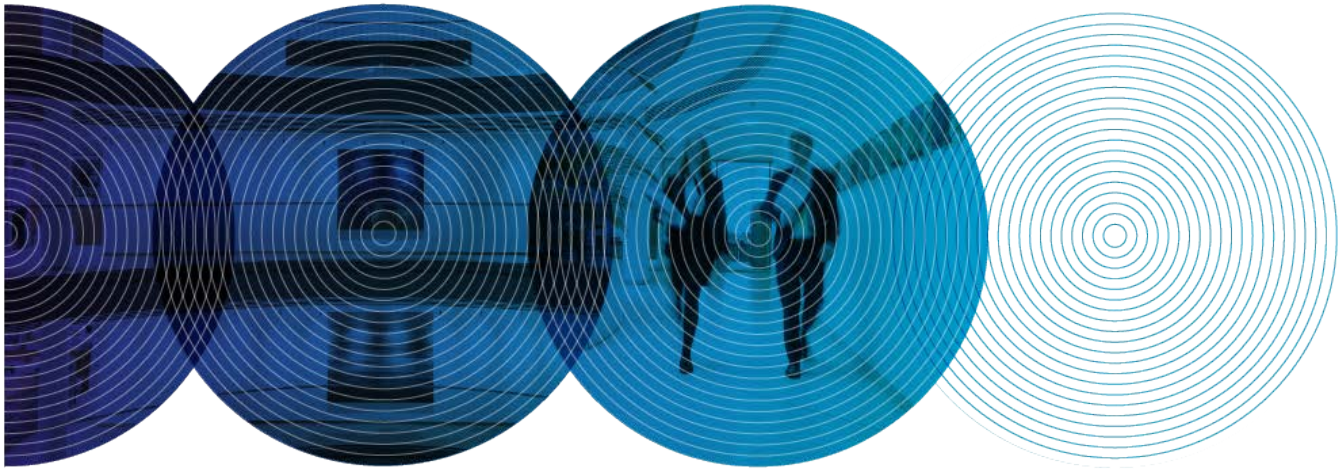
- Article 6(1) - processing necessary for one of the following purposes:
  - the performance of a contract to which the data subject is party
  - for compliance with a legal obligation imposed on the controller
  - to protect the vital interests of the data subject/other person
  - for the performance of a task carried out in the public interest or in the exercise of official authority
  - for the legitimate interests of the controller/third party – subject to fundamental rights/freedoms of data subject

Institute of Directors and McCann FitzGerald

GDPR – Areas of Concern for Irish Business

Adam Finlay, Partner, Technology & Innovation

Thursday, 1 February 2018



McCann FitzGerald

INSTITUTE OF DIRECTORS IN IRELAND

Data Inventory/Record of Processing Operations

- Record of processing mandatory for all controllers and processors, subject to limited exemption:
  - fewer than 250 employees ***and***
    - processing is not likely to result in risk to data subjects
    - processing is not occasional
    - processing does not involve special categories of data/criminal data

Records of Processing

- Mandatory for controller
  - Contact details of controller
  - DPO and Representative details, if applicable
  - Purpose of processing
  - Categories of data subject
  - Categories of personal data
  - Categories of recipient
  - Transfers outside EEA
  - Time limits for retention
  - Technical and organisational security measures

Records of Processing *cont'd*

- Optional for controller
  - details of data processors
  - legal basis for processing
  - applicable data subject rights
  - sources of data
  - *etc*

DPOs

- Do we need to appoint one?
  - public authorities
  - core activities consist of regular and systematic monitoring of data subjects on a large scale
  - core activities consist of large scale processing of special categories of data/criminal data
  - any additional local law obligation?
- If no DPO, need to document rationale? ***Accountability***

Organisation's DPO Obligations

- Ensure role meets requirements
  - properly involved in business
  - necessary resources
  - independent, no conflict
  - report to highest level of management
- Ensure person meets requirements
  - expert knowledge of data protection law & practice

Core Tasks of DPO

- Monitor compliance
- Inform and advise organisation generally and specifically on DPIAs
- Cooperate with supervisory authority (DPC)
- Single point of contact

Outline GDPR Preparation Plan

- Importance of having senior ‘buy in’
- Data protection audit
- Policies, procedures & notices
- Consider DPO appointment
- Review contracts governing processing
- Things to watch
  - regulations issued under the Data Protection Bill
  - further DPC and Art 29 WP guidance

INSTITUTE OF DIRECTORS IN IRELAND

McCann FitzGerald

IoD & McCann FitzGerald GDPR – A Director's Guide to GDPR Implementation

1st February 2018

@IoDIreland @McCannFitz #IoDEvents