INSTITUTE OF DIRECTORS IN IRELAND

McCann FitzGerald

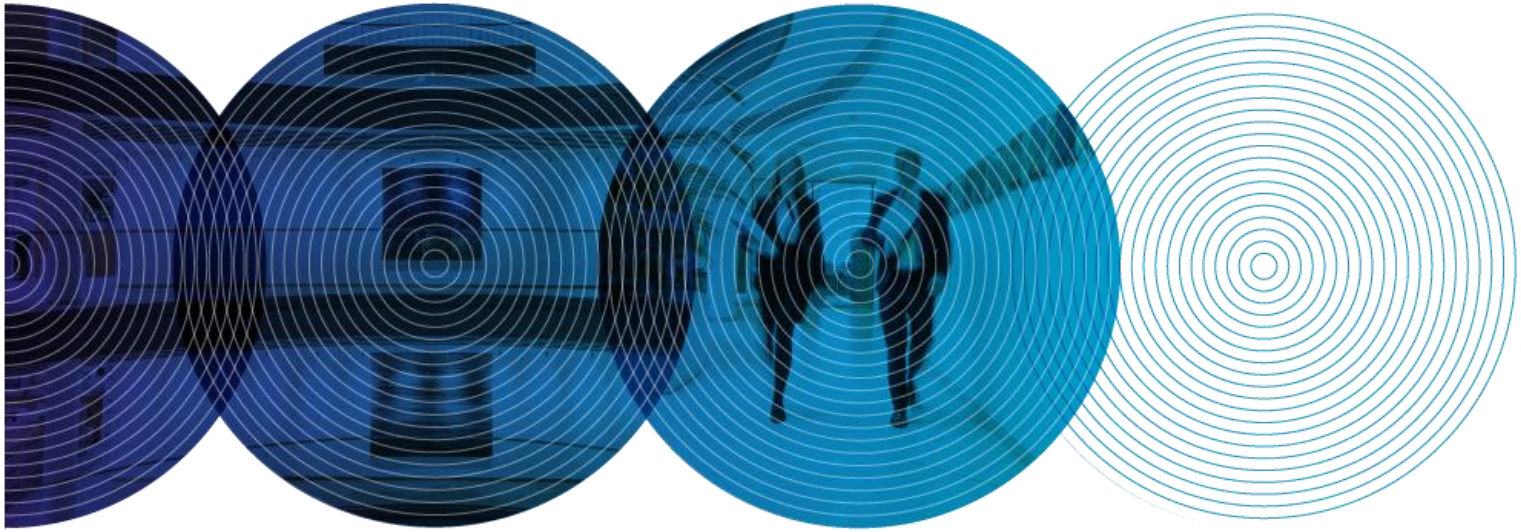
GDPR - One Year On: What Directors Need to Know

@IoDIreland
@McCannFitz #IoDEvents

IoD and McCann FitzGerald GDPR - One Year On

Paul Lavery & Adam Finlay – Technology & Innovation Group

Tuesday, 21 May 2019



McCann FitzGerald

McCann FitzGerald

Paul Lavery

Partner – Head of Technology & Innovation Group

GDPR: One Year On

- Recap – Where we are now?
- Non-Compliant Entities – what to focus on
- Materially Compliant Entities – next steps
- Developments and what to expect over the next few months
- Enforcement
- Fines

GDPR Recap

- Replaced 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
- Retained and enhanced existing data protection concepts and requirements
- Increased obligations on controllers/processors
- Afforded new rights to data subjects
- GDPR represented an "evolution" of rights and obligations, but a "revolution" in respect of administrative compliance burden and sanctions for non-compliance
- Fines – Up to €20 million or 4% of worldwide turnover

Legislative Regime

- General Data Protection Regulation
- Data Protection Act 2018
- Electronic Privacy Regulations 2011 (will ultimately be replaced by new ePrivacy Regulation)

GDPR Recap – Main Obligations

- **Fair and Transparent Processing** – *Data protection notices*
- **Legal basis for processing** - *Consent, legitimate interests, performance of contract*
- **Purpose Limitation***: Data to be kept for Specified, Explicit and Lawful Purposes and not further processed for any incompatible purposes*
- **Data Minimisation***:* Data should be adequate, relevant and not excessive
- **Obligation to keep personal data accurate and up-to-date**
- **Record Retention and Deletion:** *Obligation not to retain data for longer than necessary*
- **Transfers outside EEA:** *Prohibitions on transfers outside EEA – need to be able to rely on exemption such as consent, model clauses etc*
- **Access Rights –** *Providing copies of personal data to data subjects on request*
- **Data Security –** *Implementing and maintaining appropriate security measures against unauthorised access to, alteration, disclosure or destruction of personal data*

GDPR Recap – Main Obligations *cont.*

- **Personal Data Breach Notifications** – *Notification obligations to DPC and affected data subjects depending on whether incident is "risk" or "high risk" to data subjects*
- **Record of Processing Activities/Data Inventory** – *Recording categories of data, categories of processing activities, categories of recipients, data transfers, retention times and security measures*
- **Documenting and Evidencing Compliance** – *Drafting and implementing relevant data protection policies and information notices; privacy by default and by design; data protection impact assessments*
- **Engaging Service Providers** – *Detailed data processing provisions required to be included in contacts*
- **Increased Data Subject Rights** – *Access, rectification, erasure, data portability*

Notices and Policies - Reminder

- Notices:
  - *Data protection notice*
  - *Privacy statement on website*
- Policies
  - *General DP Policy*
  - *Data Security Policy*
  - *Breach handling and notification policy*
  - *Retention/Deletion Policy*
  - *Other policies – access request; accuracy; right to be forgotten; data portability (could be included instead in one overall internal DP Policy)*

GDPR – Where are we now?

- Post 25 May 2018 - less enforcement activity? –This has now changed – investigations and enforcement ramping up
- Broad range of preparation levels – many entities focussed on minimum needed to document and evidence compliance; others undertook significant compliance exercises
- Entities who were not adequately prepared – Focus on main compliance elements
- Entities who consider themselves materially compliant – Ensure on-going review and good house-keeping
- Compliance challenges

GDPR – Non-Compliant Entities: Document and evidence compliance

- **Data Inventory** – Description of data and purposes of processing - *what, where, why and for how long*
- **Data protection notices/Privacy statements –** Require more detail
- **Data protection policies and procedures** – Review of any existing policies and procedures and potential need for additional policies
- **Identify Legal Basis for processing –** Consent, legitimate interests etc .
- **Controller/processor agreements** – Require more detail
- **Data security breaches** – Mandatory reporting
- **Data Protection Officer –** Appointment will need to be considered. Ensure appropriate support and potential need to enshrine guaranteed independence in role

GDPR – Materially Compliant Entities: Ongoing review and housekeeping

- **Governance –** Implement governance structure to ensure that GDPR remains a compliance priority (data protection champion or Data Protection Officer?)
- **Regular review** of documents, policies and notices (yearly?)
- **Guidance -** Keep an eye out for further European Data Protection Board and DPC guidance
- **Controller/processor agreements** – Most entities have not completed exercise of updating all contracts with service providers
- Where relying on legitimate interests – carry out and document **legitimate interest balancing test**
- **Privacy Impact Assessments and Data Protection Impact Assessments**
- **Retention and destruction policies**

What Now?

- Increased number of DPC audits/investigations
- Fines – DP Authorities will need to find their feet, ascertain appropriate fines – likely to be a "wobbly period" –significant number of appeals?
- Discovery of unintended consequences of GDPR and/or Data Protection Act that need to be rectified – potential that regulations will be drafted to facilitate processing of different categories of data
- Prospective new ePrivacy Regulation - marketing

What Now – DPC Enforcement Priorities

- Increased DPC audits, investigations and enforcement
- Primarily directed by complaints and breach notifications but DPC also empowered to commence investigations at its own instance
- DPC Focus on public and private sector organisations involved in large scale, high risk processing including:
  - *Intensive tracking and profiling*
  - *Online internet platforms*
  - *Processing of health or biometric data*
  - *Finance and insurance data*
  - *Emerging technologies (IoT or AI)*
  - *Automated decision making and profiling*
  - *Global Privacy Enforcement Network – Letters sent to certain companies including pharma company in Ireland*

McCann FitzGerald

Adam Finlay

Partner – Technology & Innovation Group

What Does Enforcement Look Like?

- Data Protection Authorities
  - *Corrective action – fines and/or binding orders*
  - *Criminal enforcement*
- Data Subjects
  - *Complaints*
  - *Data protection actions*
- Representative bodies
  - *Exercising data subject rights*

Enforcement – Data Protection Commission

- 52 open inquiries, of which 17 relate to tech MNCs
- 7 own-volition investigations arising from personal data breach notifications*
- Corrective powers
  - *Warnings, reprimands, orders, suspensions, bans*
  - *Fines - effective, proportionate and dissuasive (none by DPC yet)*

Fines by other DPAs

- France – €50million – Google Inc. fines for failures in respect transparency and inadequate consents
- Austria – €4,800 – Use of CCTV to monitor public area deemed excessive, no notices put in place
- Portugal – €400,000 – Hospital's failure to limit access to data and inability to demonstrate it had appropriate security measures in place
- Germany – €20,000 – Hackers stole 330,000 user email addresses and passwords that were kept in plain text

Fines by other DPAs

- Hungary – €35,000 – Database containing details of political party's supporters (circa 6,000 people) accessible on hacker forum due to poor security measures
- Poland – €200,000 – Failure to provide transparency notices by company that aggregated publicly available data
- Denmark – €160,000 (2.8% turnover) – Taxi company deleted customer names and addresses after 2 years, but retained phone numbers for a further 3 years

Fines – Aggravating and Mitigating Factors

- Nature, gravity and duration
- Intentional or negligent
- Any action to mitigate damage
- Degree of responsibility, taking into account technical and organizational measures
- Previous infringements or enforcement actions
- Degree of cooperation with supervisory authority
- Categories of personal data affected
- How infringement became known to supervisory authority
- Adherence to approved codes of conduct
- Any other aggravating or mitigating factor, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement

Enforcement – Data Subjects

- Complaints to DPC generally arise from data subject requests or personal data breach notifications
  - *34% of complaints related to access requests**
  - *5,500 personal data breaches notified to date*
    - 250 deemed high risk and data subjects notified
    - 120 related complaints
- Data protection actions
  - *Circuit Court and High Court actions – what compensation if no material damage?*

Enforcement – Representative Bodies

- NOYB, La Quadrature du Net, etc.
- Varying motives

Questions?

McCann FitzGerald

Principal Office
Riverside One, Sir John Rogerson's Quay
Dublin 2 D02 X576
+353 1 829 0000

New York
Tower 45, 120 West 45th Street, 19th Floor
New York, NY 10036
+1 646 952 6001

London
Tower 42, Level 38C, 25 Old Broad Street
London EC2N 1HQ
+44 20 7621 1000

Brussels
40 Square de Meeûs, 1000 Brussels
+32 2 740 0370

INSTITUTE OF DIRECTORS IN IRELAND

McCann FitzGerald

GDPR - One Year On: What Directors Need to Know

@IoDIreland
@McCannFitz #IoDEvents