# GDPR FOR PENSION TRUSTEES

Annette Hogan
McCann FitzGerald

McCann FitzGerald

# New Regime

- EU General Data Protection Regulation
  - Directly applicable in all Member States - 25 May 2018
  - Single uniform set of data protection rules across the EU
  - Will replace Data Protection Acts 1988 and 2003
- Proposal for e-Privacy Regulation
  - Will replace Electronic Privacy Regulations (SI 336/2011)

McCann FitzGerald

# Similar Basic Principles

- Fair collection and processing; legitimising processing
- Specified, explicit and legitimate purposes
- Adequate, relevant and not excessive;
- Accurate and up-to-date; not keeping for longer than necessary
- Higher obligations for special categories of data
- Appropriate security measures
- Subject access rights
- Contracts with data processors
- Restrictions on transfer outside the EEA

McCann FitzGerald

# Key Changes

- Data protection notices - more detailed information to be provided
  - E.g. retention period, right to withdraw consent, legitimate interests being relied on, data subject rights, etc.
- Consent
  - Freely given, specific, informed and unambiguous
  - Should not be bundled with other consents
  - 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
- Legitimate interests - no longer available to public authorities

McCann FitzGerald

# Key Changes

- Increased internal governance
  - Removal of registration obligation
  - Replaced with obligation to adopt internal policies demonstrating compliance
  - Privacy Impact Assessments
- Increased data subject rights
  - Right of access and rectification – no fee
  - Right of erasure ("right to be forgotten")
  - Data portability – to data subject or new data controller
    - processing based on consent/contract with data subject
    - automated data only – Art 29 WP "observed data"

McCann FitzGerald

# Key Changes

- Contracts with data processors – more detailed clauses to be included
  - E.g. consent to appointment of sub-processors, notification of security breach, return/deletion of data, audit, back to back contracts with sub-processors, etc.
- More severe financial penalties
  - Up to 4% of annual worldwide turnover of 'undertaking' or €20 million (whichever is greater)
  - Fines may be levied by Data Protection Authorities themselves
- Data Protection Officer
  - Public authorities
  - Regular and systematic monitoring of data subjects on a large scale
  - Large scale processing of special categories of data

McCann FitzGerald

# Key Changes

- Personal data security breach – 72 hour notification
- Lead supervisory authority – "One Stop Shop"
  - Place of main establishment of controller or processor
- Extra-territorial effect
  - controllers and processors outside EU which target EU data subjects

McCann FitzGerald

# Internal Governance – Policies and Notices

- Data Inventory
- General Data Protection Policy
- Data Security Policy
- Breach Notification Policy
- Record Retention Policy
- Access Request Policy
- Other potential policies – accuracy, data deletion, data portability, etc.
- Data Protection Notices to data subjects
- Data protection provisions in employee handbook
- Privacy Impact Assessments

McCann FitzGerald

# Preparing for GDPR

- Get senior ‘buy in’
- Data protection audit
- Policies, procedures & notices
- Consider DPO appointment
- Review contracts governing processing
- Keep an eye out for Data Protection Bill and DPC and Art 29 WP guidance

McCann FitzGerald