GDPR Update

Four week reflection

IIPM
Irish Institute of Pensions Management

What has been happening?

- 25th May has passed
- GDPR is operational
- Data Protection Act 2018 passed (24th May)
- Limited exception for sensitive data
- Pensions Authority issued guidance
- Everybody has their act in order?
- Time to reflect

IIPM
Irish Institute of Pensions Management

What is your role?

- Trustee?
- Provider/Life Office?
- Registered Administrator?
- Broker/Consultant/Adviser?
- Auditor?
- Employer/Staff of Employer?

Data Controller?

Data Processor?

- Do you have access to or handle data?

IIPM
Irish Institute of Pensions Management

Processing

- Any operation or set of operations
- performed on personal data or on sets of personal data
- whether or not by automated means
- such as

- ❖ Collection
- ❖ Recording
- ❖ Organisation
- ❖ Structuring
- ❖ Storage
- ❖ Adaptation
- ❖ Alteration
- ❖ Retrieval
- ❖ Consultation
- ❖ Use
- ❖ Disclosure by transmission
- ❖ Dissemination
- ❖ Otherwise making available
- ❖ Alignment or combination
- ❖ Restriction
- ❖ Erasure or destruction

Article 4(2)

IIPM
Irish Institute of Pensions Management

Data Controller

- **Determines the purposes and means of processing**

Article 4(7)

- Risk based measures (likelihood and severity)
- Data Protection by design
- Technical and organisational measures
- Demonstrable
- Approved Codes

Articles 24 & 25

IIPM
Irish Institute of Pensions Management

Multiple Controllers?

- Trustees are Controllers (always?)
- Life Offices, RAs, Consultants identifying as Controllers
- Determine the purposes and means of processing?

- Joint controllers
- Transparent, agreement, disclosure

- Possibility of two Controllers, but not Joint?

IIPM
Irish Institute of Pensions Management

Article 26 *Section 79*

Processor

- Processes **on behalf of Controller**

Article 4(8)

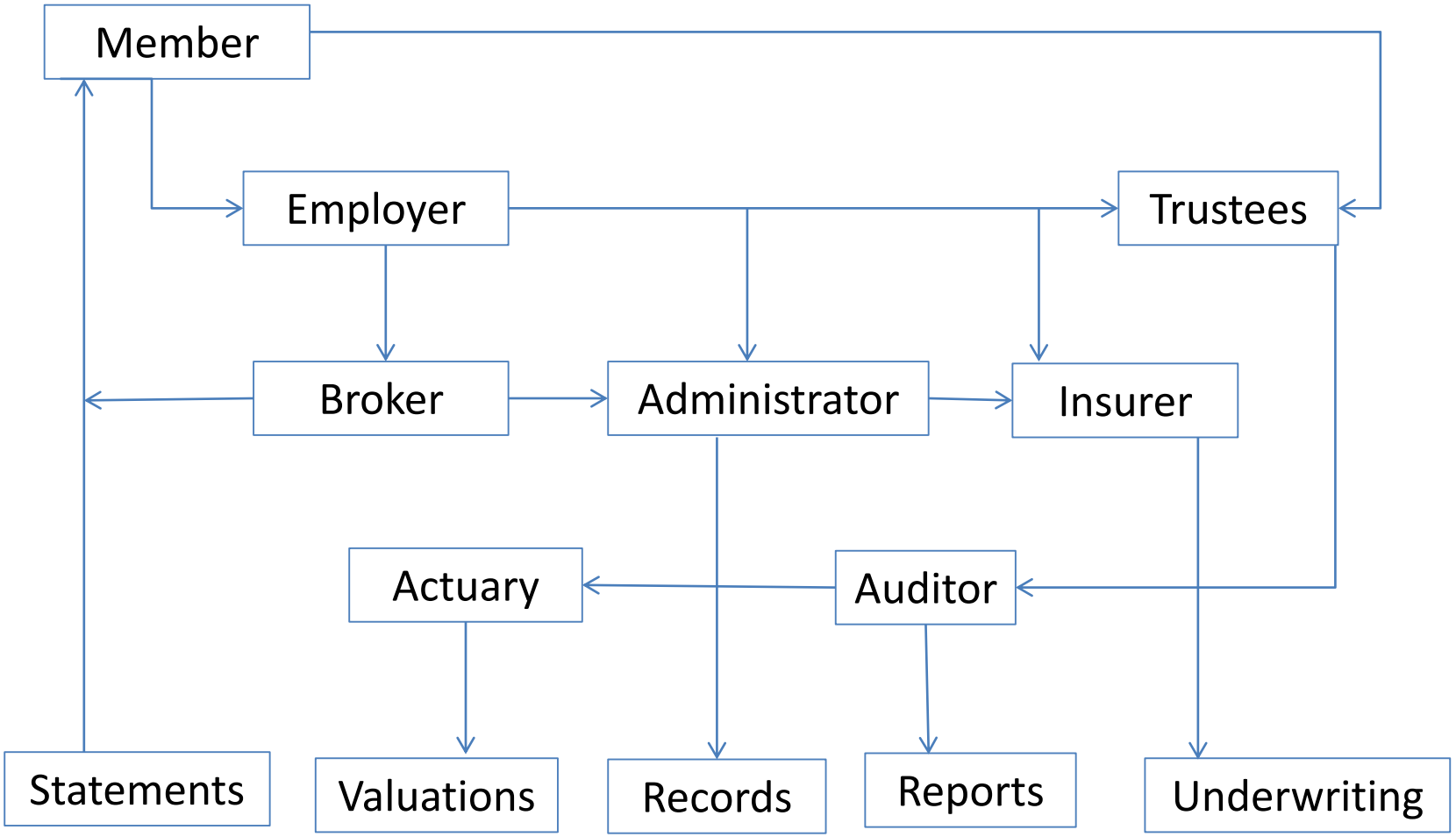
- Personnel committed
- Appropriate measures for protection of data
- Legal contract, documented instructions
- Confidentiality and Security
- Sub-processor, secondary processor
- Cooperation with Controller
- Commission, Regulator may specify some contractual terms

IIPM
Irish Institute of Pensions Management

Articles 28 & 29

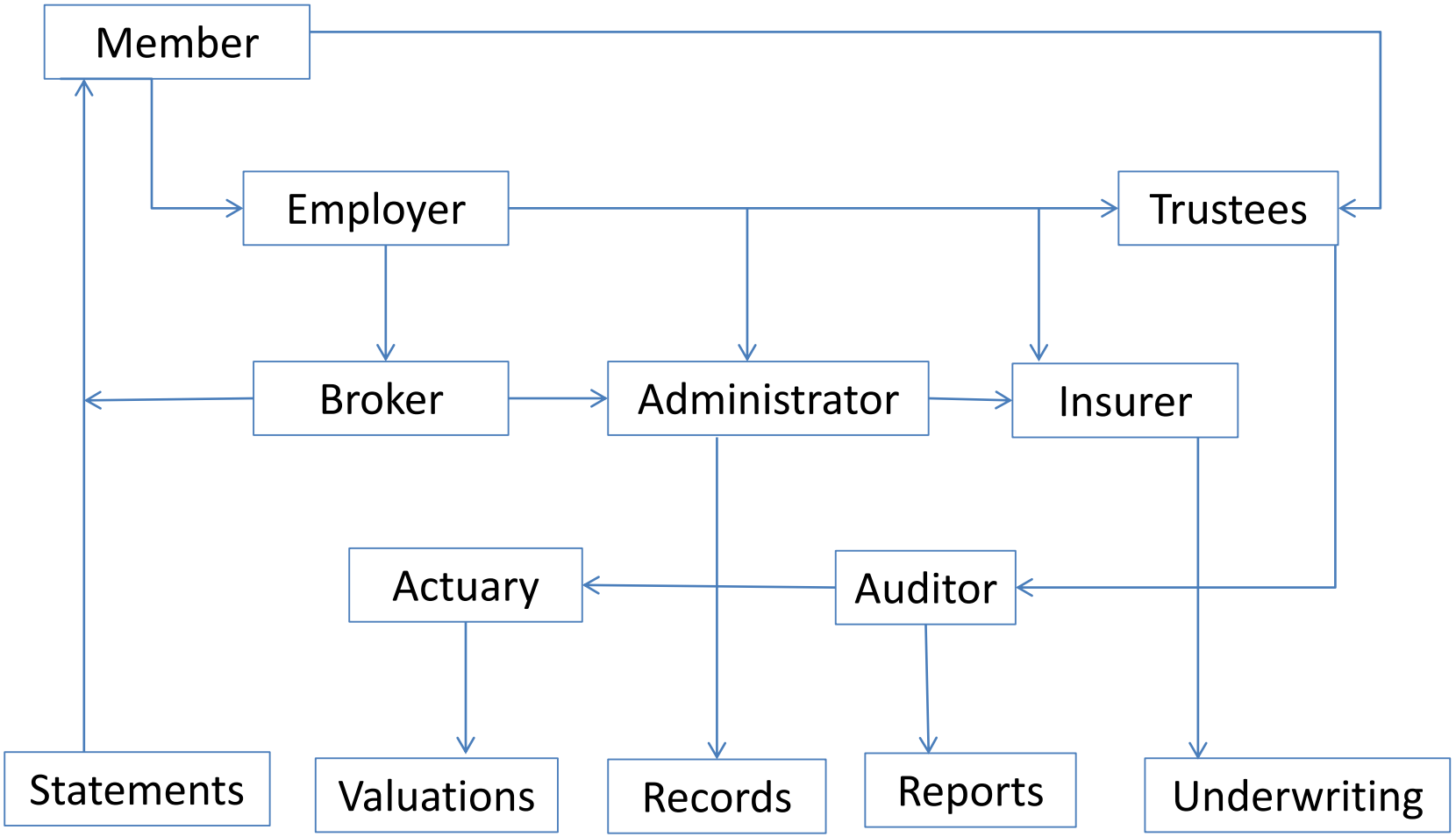
Section 80

Data Mapping



IIPM
Irish Institute of Pensions Management

Who are Controllers/Processors?



IIPM
Irish Institute of Pensions Management

Agreements

- Trustees appoint everyone?
- Everyone a Processor on behalf of Trustees?
- Controller to Controller?
- Joint Controller arrangements?
- Controller to Processor – specific, in writing
- Existing contracts adequate?
- Position of Employers?
- Whose responsibility?

IIPM
Irish Institute of Pensions Management

Data Privacy Notices

- At the time of receipt from member
- Within 1 month if received from other source
- Existing members?

Articles 13 & 14

- Already a plethora of DPNs going to members
- Each Controller has the obligation

- Have DPN ready for new entrants
- Existing members asap
- At next communication (e.g. benefit statements)?
- Post on website?
- Former members are data subjects too

IIPM
Irish Institute of Pensions Management

Data Privacy Notices

- Identity of Controller, contact details
- Data Protection Officer, if any
- What data is being held
- If received from individual
- If not, from whom
- Reason/justification
- How long it will be held
- With whom will it be shared
- If transferred outside EEA & protection measures
- Information on other rights & mechanism for exercising

Articles 13 & 14

IIPM
Irish Institute of Pensions Management

Data Protection Officer

- Do you need one?
- Applies to Controllers and Processors
- If core activities consist of regular and systematic monitoring of data subjects on a large scale
- Or large scale of special categories of data
- Specific rules regarding DPO appointment, independence and functions
- Other person, but not formal DPO?

IIPM
Irish Institute of Pensions Management

Article 37

Sensitive Data

- Special Categories
  - racial or ethnic origin
  - political opinions
  - religious or philosophical beliefs
  - trade union membership
  - genetic data, biometric data for the purpose of identification
  - data concerning health
  - data concerning a person's sex life or sexual orientation
- Processing prohibited – unless express consent
- Or as specified by Data Protection Act
  - Health in context of pensions and insurance *s. 50*
  - Other if required for employment rights *s. 45*
  - Subject to *Suitable and Specific* measures *s. 36*

IIPM
Irish Institute of Pensions Management

Suitable and Specific Measures

- Measures may include
  - Consent for specified purpose
  - Limited access in workplace
  - Strict time limits
  - Targeted training
  - Logging, tracking, verification of access
  - Data Protection Officer (even if not required)
  - Limited to health professional, or person with equivalent duty
  - Pseudonymisation, encryption
- Minister may specify measures, governance structures
- Do you process Special Categories?
- Measures in place?
- Purpose, justification?
- Family information still problematic

IIPM
Irish Institute of Pensions Management

Access Requests

- Anecdotal so far
- Cranks' charter?
- Thirty days almost up
- Share feedback on experiences

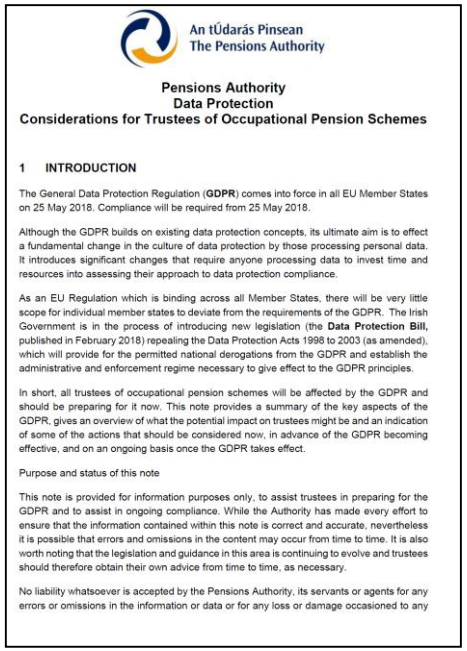
IIPM
Irish Institute of Pensions Management

Where Does This Leave Trustees?

- Industry has looked after its own concerns
- Many Trustees/Trustee Boards are reliant on advisers
- Do they know they are Controllers?
- Data Protection Policies?
- Contracts with Processors?
- Data Privacy Notices?
- Utilise work done by other Controllers?
- Role of Professional Trustees?
- Budgets?
- Guidance

IIPM
Irish Institute of Pensions Management

Pensions Authority



An tÚdarás Pinsean
The Pensions Authority

Pensions Authority
Data Protection
Considerations for Trustees of Occupational Pension Schemes

1 INTRODUCTION

The General Data Protection Regulation (**GDPR**) comes into force in all EU Member States on 25 May 2018. Compliance will be required from 25 May 2018.

Although the GDPR builds on existing data protection concepts, its ultimate aim is to effect a fundamental change in the culture of data protection by those processing personal data. It introduces significant changes that require anyone processing data to invest time and resources into assessing their approach to data protection compliance.

As an EU Regulation which is binding across all Member States, there will be very little scope for individual member states to deviate from the requirements of the GDPR. The Irish Government is in the process of introducing new legislation (the **Data Protection Bill,** published in February 2018) repealing the Data Protection Acts 1998 to 2003 (as amended), which will provide for the permitted national derogations from the GDPR and establish the administrative and enforcement regime necessary to give effect to the GDPR principles.

In short, all trustees of occupational pension schemes will be affected by the GDPR and should be preparing for it now. This note provides a summary of the key aspects of the GDPR, gives an overview of what the potential impact on trustees might be and an indication of some of the actions that should be considered now, in advance of the GDPR becoming effective, and on an ongoing basis once the GDPR takes effect.

Purpose and status of this note

This note is provided for information purposes only, to assist trustees in preparing for the GDPR and to assist in ongoing compliance. While the Authority has made every effort to ensure that the information contained within this note is correct and accurate, nevertheless it is possible that errors and omissions in the content may occur from time to time. It is also worth noting that the legislation and guidance in this area is continuing to evolve and trustees should therefore obtain their own advice from time to time, as necessary.

No liability whatsoever is accepted by the Pensions Authority, its servants or agents for any errors or omissions in the information or data or for any loss or damage occasioned to any

- Principles
- Definitions
- Design and Default
- DPIA
- Register of Processing
- Processor Contracts
- DPOs
- Legal Basis
- Communication
- Access Requests
- Individual Rights
- Breaches
- Data Protection Officer
- International Transfers

IIPM
Irish Institute of Pensions Management

https://www.pensionsauthority.ie/en/Trustees_Registered_Administrators/Guidance/Information_note_on_data_protection_for_trustees_of_occupational_pension_schemes_-_May_2018.pdf

Action Points For Trustees

- Identify who is responsible
- Data mapping
- Register of data and processing
- Compliance plan
- Monitoring and awareness

- Identify legal basis

- Review and amend DPN
- Issue revised DPNs

- DPO, or Reasons why not

- Review access procedures
- Templates for response

- Inform members of rights
- Amend systems

- Review security measures
- Encryption

- Breach procedures
- Review processor agreements

- Systems for deletion/rectification

IIPM
Irish Institute of Pensions Management

Trustees' Key Documents

- Data Privacy Notice
- Trustees' Data Protection Policy
- Data Breach Procedure
- Agreements with Processors
- Other Controllers? Joint Controllers?

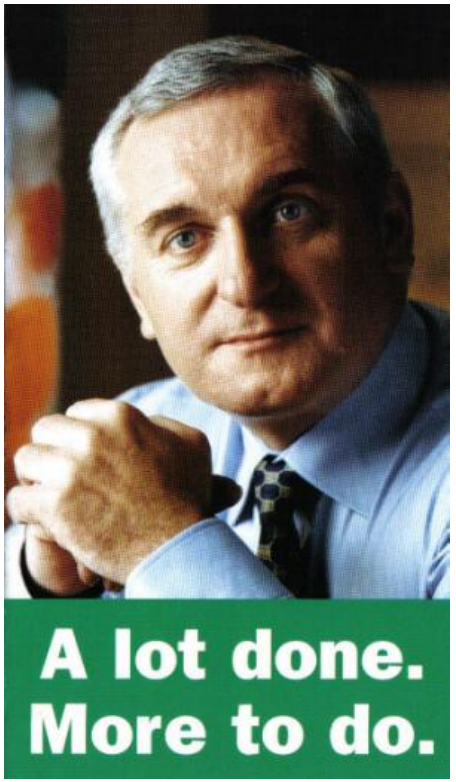
- Amendments to existing supplier agreements or terms of business
- Data processing record
- Data mapping
- Data Protection Impact Assessment
- What other documents ?

IIPM
Irish Institute of Pensions Management

And Finally…

- Brave new world
- Not all that different from the old one
- A bit more formalised and structured

- No matter how well you have been prepared
- Or how poorly
- Time to reflect, consolidate
- We are the good guys
- Make it show



IIPM
Irish Institute of Pensions Management