General Data Protection Regulation ("GDPR") and Pensions

Olivia Mullooly, Technology and Innovation
Sarah McCague, Pensions
28 November 2019

ARTHUR COX

Overview

- GDPR 18 months in
- IAPF Guidance – a review
- Reporting and enforcement landscape
- GDPR and IORP II

Key terms – a recap

- ***Data controller*** **– controls personal data (determines the purpose and means of the processing)**
- ***Data processor*** **– processes personal data on behalf of the controller**
- ***Data subject*** **– the identifiable person to whom the personal data relates**
- ***Personal data*** **– any information relating to a data subject (i.e. from which indent of an individual can be ascertained)**
- ***Special categories of personal data*** **– includes race, ethnicity, religious beliefs, trade, union status, sexual orientation, health data, among others**

18 months in – where are we?

- Came into effect on 25 May 2018
- Much public awareness
- Pensions liaison officer appointed by DPC
- Transparency notices (for the most part) issued
- Core GDPR documents agreed
- 3rd party clauses agreed?

IAPF Guidance

- The Guidance:
  - *Prepared to provide clarity*
  - *Prepared on the basis that trustees are controllers and service providers are processors or sub-processors*
  - *But note - service providers may be joint controllers*
- Not a Code of Conduct
- Trustees or administrators may still need to seek legal advice
- Part A – overview Part B - Guidance

IAPF Guidance (Part B)

1. **Identify Controller, Processors, Sub-Processors and any Joint Controllers**
   - *Identify respective roles (obtain advice if not clear)*
   - *Enter legal agreements*

2. **Controller to put in place Data Privacy Notice for Data Subjects**
   -annual benefit statement
   - application form
   - scheme website/benefits dashboard

3. **Controller identify Personal Data processed and legal basis**
   -what Personal Data is being processed, why and for how long
   - legal bases for processing

IAPF Guidance (Part B)

4. **Controller to put in place Data Protection Policy and a Data Retention Policy**

   - prepare based on 7 principles

   - all relevant persons required to comply with policy

   - cross-refer to other polices

5. **Controller and Processor enter into binding legal agreements re GDPR obligations**

   -include minimum contractual commitments required by GDPR

   -confirm sub-processors are contractually bound by commitments

   -consider joint controller agreements

IAPF Guidance (Part B)

6. **Controller to adopt a Data Breach Policy and keep a Data Breach Register**
   - *assists trustees in meeting personal data breach requirements of GDPR*
   - *ensure 3rd party processors are aware and will comply*

7. **Controller to adopt a Data Security Policy**
   - *no personal email accounts*
   - *strong passwords*
   - *portable electronic devices encryption*
   - *encrypt email*
   - *secure disposal*

8. **Controller to adopt Subject Request Procedure and keep a Data Subject Request Register**
   -procedure: by whom, when, how, fees, format of replies, time limits
   - register: all data subject requests and responses issued

Data breach reporting landscape

- When should you report to DPC?
- When should you notify member?
- Types of breaches being reported
- Enforcements by DPC

GDPR and IORP II

- IORP II transposition date 13 January 2019
- Awaiting implementing legislation
- GDPR relevant:
  - Disclosure requirements - *public disclosure of annual accounts and reports*
  - Deferred members – *annual statements and data verification*
  - Governance manual and checklist

Thank you