

GDPR AND PENSIONS

ASSOCIATION OF CONSULTING ACTUARIES

SARA CHAMBERS

21 MAY 2018



GOWLING WLG

DATA PROTECTION AND PENSIONS



GDPR will go into direct effect across the EU on 25 May 2018



The UK will also have a new Data Protection Act 2018



Data processors will have direct legal duties as well as data controllers.



The maximum fine will be the higher of:

- **€20 million; and**
- **4% global turnover.**

TERMINOLOGY REMINDER

CONTROLLER

Trustee
Employer
Actuary
Lawyer

PROCESSOR

Administrator
Investment
consultants

PERSONAL DATA

Updated definition of
personal data in the
GDPR

PROCESSING

Anything you will
do with data

DATA SUBJECT

Scheme members
Beneficiaries



GOWLING WLG

CONTROLLERS AND PROCESSORS



GOWLING WLG

DATA PROTECTION PRINCIPLES

ACCOUNTABILITY

Processed lawfully,
fairly and in a
transparent manner

Collected for
specified, explicit
and legitimate
purposes

Adequate, relevant
and limited to what
is necessary

Accurate and kept
up to date

Retained for no
longer than is
necessary

Processed in a
manner to ensure
appropriate security

CONTROLLERS AND JOINT CONTROLLERS

- A “Controller” determines the purposes and means of processing personal data
- “Joint controllers” where two or more Controllers jointly determine the purposes and means of processing
- GDPR requires Joint Controllers (i.e. actuarial firm / scheme actuaries and pension trustees) to agree their respective responsibilities.
- Essence of agreement should be made available to data subjects
- Data subject may exercise rights under GDPR against either Controller



DATA PROCESSORS

- Data Controllers must only use Data Processors which provide **sufficient guarantees** to implement appropriate technical and organisational measures
- Data Controllers must have **contractual terms** in place with Data Processor setting out
 - the subject matter and duration, nature and purpose of processing
 - type of personal data and categories of data subjects
 - obligations and rights of the controller
 - meet the requirements of article 28 including requirements for confidentiality, use of sub-processors, assistance with compliance, audit etc



PRIVACY NOTICES



GOWLING WLG

PRIVACY NOTICES

- The trustee of a pension scheme is responsible for a Scheme's privacy notice
- Privacy notice must include
 - What personal information held
 - How it is obtained
 - What it is used for
 - What the grounds for processing it are
 - Whether there are multiple data controllers
 - Details about member rights in respect of their data
- What information about other controllers should be included?



DATA SECURITY AND WHAT OUR CLIENTS EXPECT



GOWLING WLG

DATA SECURITY – ACCESS IDEAS

IDEAS FOR PHYSICAL ACCESS CONTROLS



Limiting access
to workspaces



Locking filing
cabinets



Secure archiving
of older documents



Secure document
disposal



Safe storage of
sensitive material



Clear desk policy



GOWLING WLG

DATA SECURITY – ACCESS IDEAS

IDEAS FOR ELECTRONIC ACCESS CONTROLS



Print controls



Password protecting
specific folders / files



Virus / malware
protection



Password complexity
and change requirements



Encryption of
computer systems



Security settings for
approved mobile devices



GOWLING WLG

SIMPLE STEPS TO HELP IMPROVE DATA SECURITY

Pseudonymisation

**Password
protection**

Replying to all

**Taking hard
copies out of the
office**

**Think before
sending email to a
personal email
address**

Secure disposal



GOWLING WLG

DEALING WITH DATA SUBJECT RIGHTS REQUESTS



GOWLING WLG

DATA SUBJECT RIGHTS

RESTRICT

**PORT-
ABILITY**

OBJECT

**ADM /
PROFILING**

ERASURE

**RECTIFICA
-TION**

ACCESS

INFORM



GOWLING WLG

DATA SUBJECT RIGHTS – KEY POINTS

Process or policy?

Responsibility for responding?

Getting help from relevant third parties

Awareness of time limits and format of responses



RISK MANAGEMENT AND BREACHES



GOWLING WLG

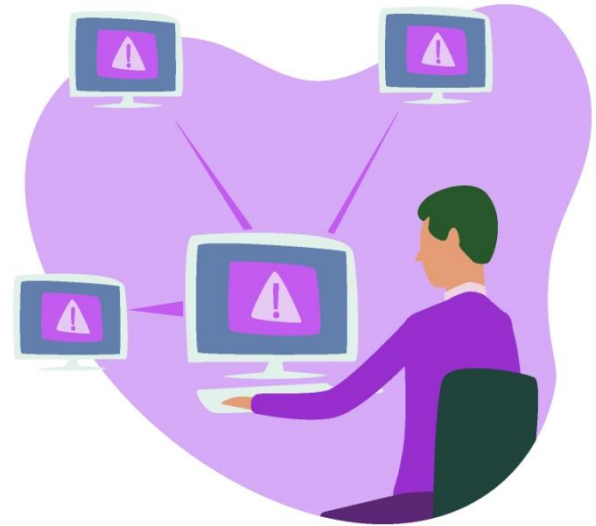
RISK MANAGEMENT - TRAINING

**Use of systems
and computers**

**Recognising
common threats**

**Recognising and
reporting
personal data
breaches**

**Policies and
procedures**



GOWLING WLG

RISK MANAGEMENT – BREACH

Personal data breach is a breach of security leading to the **accidental** or **unlawful** destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

Data Controllers need to consider how they would:

- identify;
- report;
- manage;
- resolve; and
- investigate

such breaches of the personal data they control.



BREACH REPORTING

- **Controller** to notify breaches to **ICO**
 - without undue delay and within **72 hours** if feasible unless unlikely to result in risk to rights and freedoms of individuals
 - If 72 hours not feasible must provide reasoned justification
- **Controller** to notify breaches to **data subjects**
 - without undue delay if likely to result in **high** risk to rights and freedoms of individuals
- **Processor** to notify **Controller** of breaches without undue delay



QUESTIONS?



GOWLING WLG



GOWLING WLG