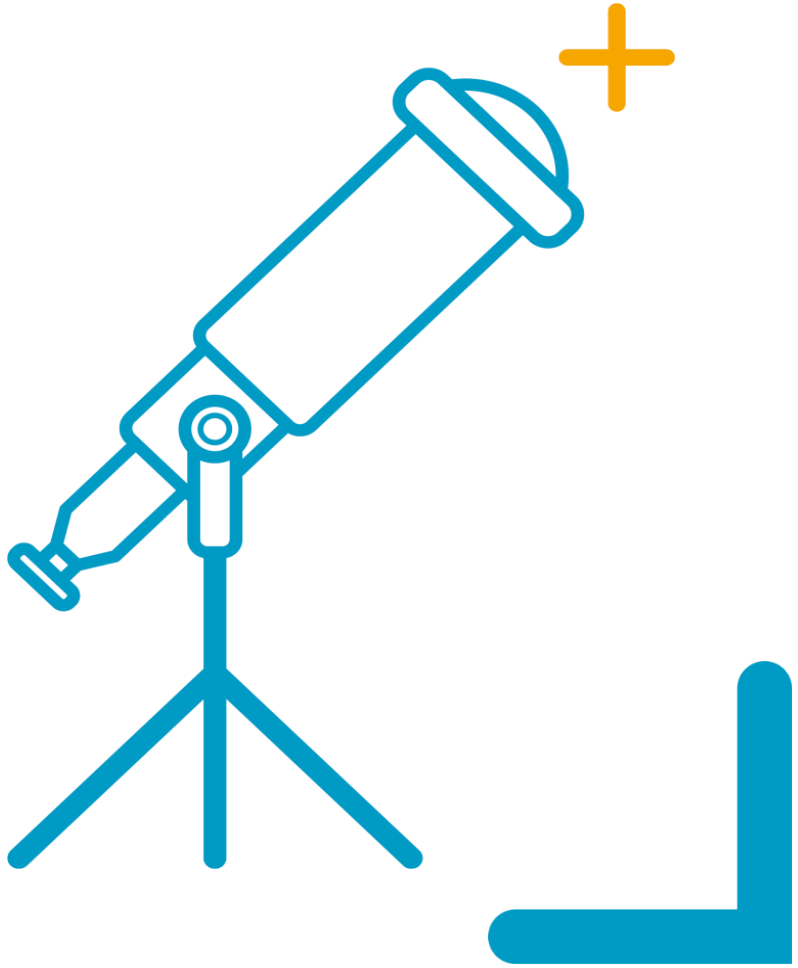
AMNT

GDPR: Key issues and actions for Trustees



Lucy Hughes

Partner

5 October 2017

General Data Protection Regulation - "GDPR"

Why Trustees need to take notice

- **Legal requirement**
- Effective from 25 May 2018
- Replaces existing data protection laws (DPA 1998)
- EU Regulation: does not need to be put into UK law
- Post-Brexit via a new Data Protection Act
- Enable data to be freely transferred between UK and EU
- **Huge fines**
- €20m or 4% of global annual turnover

Who does GDPR apply to?

- Organisations processing personal data within the EU
- Organisations outside the EU that offer goods or services to individuals within the EU

Pension schemes are no exception

- Applies to Data Controllers (eg Trustees, Scheme Actuaries)
- Data Processors (eg Pensions Administration, Investment, Employee Benefits and HR)

What information does GDPR apply to?

It's personal

- **Personal Data:** enables an individual to be identified
- GDPR's definition more detailed eg IP address
- **Special Categories of Personal Data:** "sensitive personal data" under the DPA
- Health, race, religion, political opinions, sexual orientation, genetic and biometric data
- Name of spouse could be deemed sensitive personal data
- Greater restrictions apply to this data

Key changes for Pension Schemes

What actions should Trustees take?

- Record keeping and audit trail
- Registration with the ICO
- Member consent
- Contracts
- Data protection (privacy) notices
- Sanctions and fines
- Data breaches
- Data protection officer
- Rights of individuals

Record keeping and audit trail

Where, why, how and by whom is data processed

- Under GDPR Trustees no longer need to register with ICO
- Greater record keeping requirements
  - Data held
  - Purpose
  - Who disclosed to

ACTION

- Ask processors to create a record of data they hold
- Pensions administrators, advisers, service providers, insurers

Member consent

Confirm lawful basis upon which data is processed

Member consent

- Must be freely given, specified, informed and unambiguous
- Can be withdrawn at any time
- Consider using different legal basis

Compliance with legal obligation

- eg to provide benefits in the scheme rules

Legitimate interest of Trustees

- eg to devise suitable investment strategy

ACTION

Confirm legal basis on which data is processed

Contractual protection

Data processor obligations

- Changes to obligations and liabilities for data processors
- Now similar to data controllers
- Impact third party admin providers
- Some mandatory requirements in data processor contracts

ACTION

- Review contracts with advisers, service providers, insurance companies etc
- Data processor confirm steps taking to comply with GDPR
- Review liability insurance policy

Privacy notices

What information must be given to members?

- Clear and plain language
- Right to more detailed information
- Include
  - legal basis for processing
  - How long data will be held
  - Right to complain to ICO

ACTION

- Review notices
- Agree with admin team how they will be issued

Data breaches

Fines and sanctions

- Was £500,000
- Now **€20m** or **4% of global annual turnover**, if higher
- Not clear how worldwide turnover applies to pension schemes
- Could Trustees reimburse from scheme assets?
- Failure to notify: fines of up to €10m or 2% annual global turnover

NHS

cex

DEBENHAMS

YAHOO!

EQUIFAX

TalkTalk

wonga

Data breaches

Do you know what happens if a breach occurs?

- Notify ICO within 72 hours of discovery where "*breach is likely to result in a risk to the rights and freedoms of individual data subjects*"
- Notify member "*without delay*" if "*high risk to rights and freedoms*"
- Robust breach plan: how you will respond?
- ICO issuing guidance

ACTION

- Put in place clear and robust process
- Maintain a record of any breaches
- Review technological requirements

Data Protection officer

- If local laws require it (new Data Protection Bill)
- If activities involve:
  - Regular and systematic monitoring of data
  - Processing Sensitive Personal Data on a large scale
- Does this apply to Trustees?
- If yes, who will be DPO?
- Can you share DPO with sponsoring employer

ACTION

- Consider whether DPO requirements apply (may want to wait for further guidance)

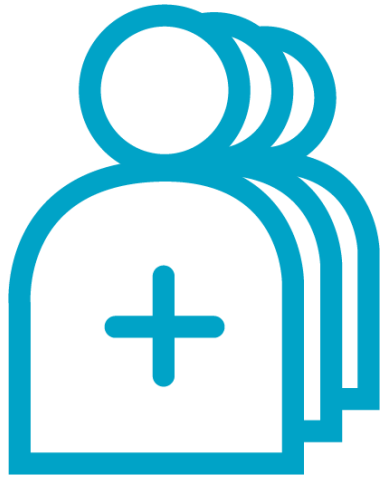
Rights of members

Subject access requests

- Must be provided within one month
- Free of charge (in most cases)
- Include period for which data will be stored
- May occur when complaint has failed

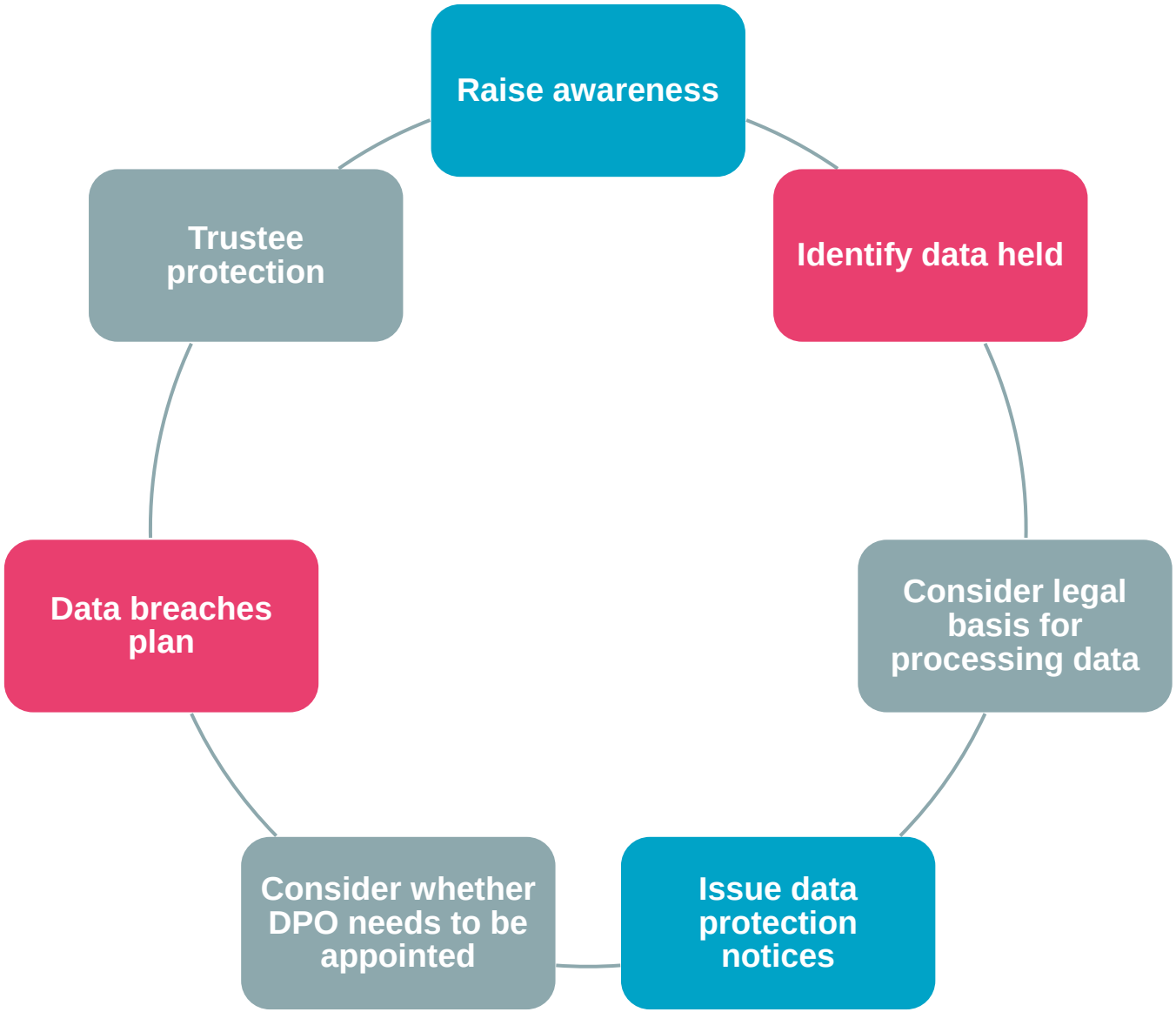
ACTION

- Review and update plan for dealing with SARs



Actions for Trustees to take

Raise this with your committees and boards



Contact us

Your AMNT Relationship Director

Lorraine Porter

Client Development Director

020 7432 3066

lorraine.porter@lcp.uk.com

Use of our work

Lucy Hughes

Partner

lucy.hughes@lcp.uk.com

5 October 2017

Our experts work in pensions, investment, insurance, energy and employee benefits.

Join us at our next event
www.lcp.uk.com/events

Share our insights and opinions on our viewpoint
www.lcp.uk.com/our-viewpoint

Watch and listen to our comments on topical issues
Our YouTube channel

Connect with us for updates
@LCP_actuaries

LinkedIn