Data challenges in the pensions landscape and GDPR

The view from the regulator

The Pensions Regulator

On the importance of data

- *We are in the information business. We generate information to help people make choices, information to help companies know how much to pay in contributions, and information to help us sort out who manages schemes well and who doesn't.*

  Margaret Snowdon, PASA Chair and TPR NED

- Accurate records are key to ensuring
  - the right members get the right benefits at the right time,
  - accurate valuations and calculation of the cost cap

- Poor data integrity has a real impact on members

The Pensions Regulator

What are the challenges facing pension schemes?

- Major data projects
  - GMP reconciliation
- Member engagement
  - Online access
- Enhanced requirements and focus
  - **Regulator focus inc reporting requirements**
  - Money laundering regulations (June 17)
  - **GDPR (May 2018)**
  - Dashboard

The Pensions Regulator

GDPR

- General Data Protection Regulation applies from 25 May 2018
  - Brings consistency across the EU
  - Strengthens provisions of current data protection
    - Stronger individual rights (new right to data portability)
    - New obligations on data processors
  - 72 hour reporting *if a breach is likely to result in a risk to people's rights and freedoms*
  - Greatly enhanced fines available to the ICO
  - Will remain after we leave the EU
- Data Protection Bill
  - Will replace 1998 Act
  - Some implementation of GDPR, but other aspects.
  - Pension scheme 'exception'

The Pensions Regulator

Regulation – direct effect on all member states (unlike directive which needs transposing)

Individual rights – most in existence but strengthened:

- the right to be informed;
- the right of access;
- the right to rectification;
- the right to erasure;
- the right to restrict processing;
- the right to data portability;
- the right to object; and
- the right not to be subject to automated decision-making including profiling.

Data portability - obtain and reuse their personal data for their own purposes across different services: move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability

Fines – from £500K to a maximum fine of €10 million/2% of annual worldwide (group) turnover, whichever is greater (minor breach); max of €20 million or 4% of annual worldwide (group) turnover, whichever is greater (major breach)

What is the difference between the DP Bill and the GDPR?

GDPR already in effect. Some limited opps to make provisions for how applies – DPB delivers this.

Also:

- processing that does not fall within EU law, for example, where it is related to immigration.

-Implements EU law enforcement directive

- application of international data protection standards to intelligence services.

A specific easement is also proposed for occupational pensions, which is designed to allow sensitive personal data to be processed without consent where the processing:

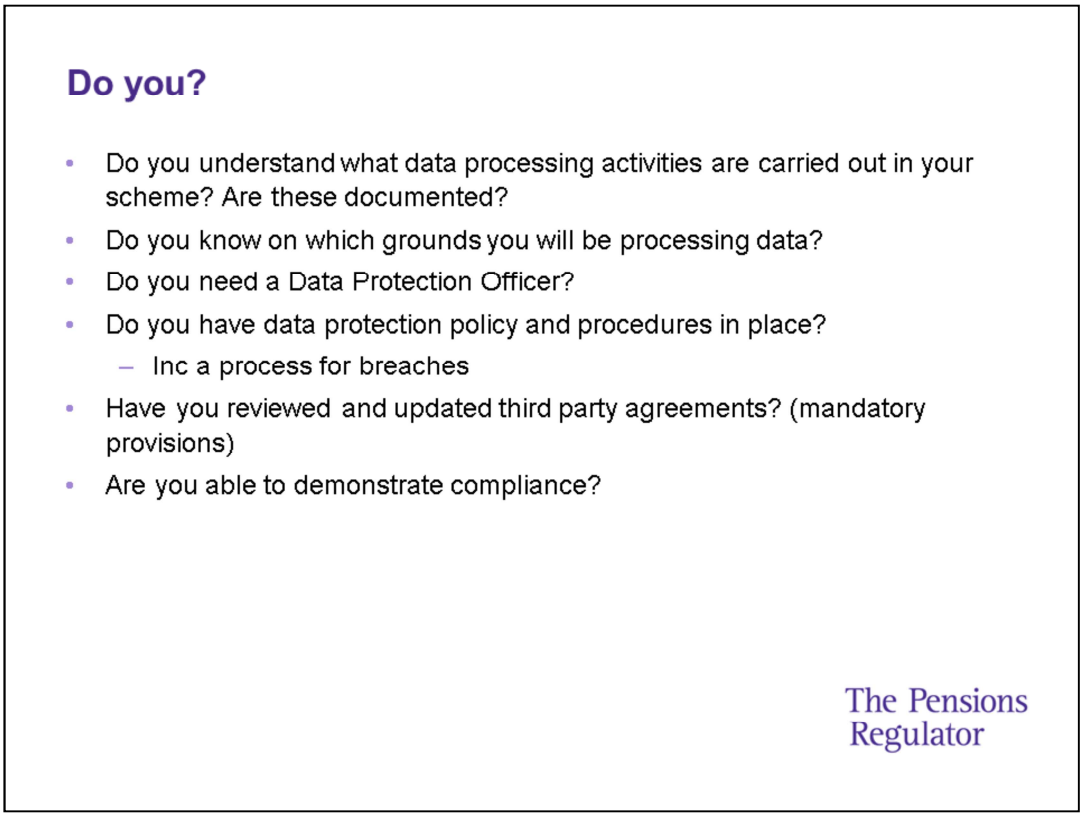
- is necessary for the purposes of making a determination in connection with eligibility for, or benefits payable under, an occupational pension scheme

- is not carried out for the purposes of measures or decisions with respect to the data subject, and

- “can reasonably be carried out without the consent of the data subject”.

For the latter test to be met, the data controller “cannot reasonably be expected” to obtain the data subject’s consent and must not be aware of the data subject withholding consent.

Could be intended to help deal with sensitive personal data which may be held incidentally in respect of potential beneficiaries (for example, on death benefit nomination forms) or other historic information such as decisions relating to past-ill health cases.



Processing data – 4 grounds.

•Conducted with the consent of the data subject

•Necessary for the performance of a contract to which the data subject is a party

•Necessary for compliance with a legal obligation to which the data controller is subject

•Necessary for the purposes of the legitimate interests pursued by the controller

Mandatory provisions - That contract or other legal act shall stipulate, in particular, that the processor:
a. processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;

b. ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

c. takes all measures required pursuant to Article 32

d. respects the conditions referred to in paragraphs 2 and 4 for engaging another processor;

e. taking into account the nature of the processing, assists the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III

f. assists the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 taking into account the nature of processing and the information available to the processor;

g. at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data;

h. makes available to the controller all information necessary to **demonstrate** compliance with the obligations laid down in this Article and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.

The good news

"If you are already complying with the terms of the Data Protection Act, and have an effective data governance programme in place, then you are already well on the way to being ready for GDPR" - Steve Wood, Deputy Commissioner for Policy, ICO

- Controls put in place for GDPR help you meet your internal controls requirements under pension legislation

The Pensions Regulator

Useful links on GDPR

- ICO - 12 steps to preparing for the GDPR
- ICO - myth-busting blog
- ICO - overview of the GDPR (evolving page)

- Industry guides also being published eg
  - PLSA guide
  - LGPS briefing

- DCMS Data Protection Bill factsheet

The Pensions Regulator

TPR focus

- Top risk for PS schemes and key focus (corporate priority)
- Our expectations
  - Governance:
    - Know & understand your duties
    - Appropriate focus/priority
    - Appropriate internal controls
      - Administrators
      - Employers
      - Data security
  - Data review
  - Robust improvement plans

The Pensions Regulator

21% FPS respondents identify poor records as a top risk; valuations – 20-25% data unacceptable

What does this mean in practice?

- Know & understand your duties
  - Pension legislation and other
  - TPR code/guidance
  - Accountability cannot be delegated
- Appropriate focus/priority
  - Administration and record-keeping seen as lower priority
  - Large schemes much more likely to feature admin on the agenda
  - Special projects (GMP, administrator switch) drive focus

The Pensions Regulator

Appropriate focus/priority

Administration and record-keeping seen as lower priority (RK qual and quant research 2016)

Large schemes much more likely to feature admin on the agenda (DC schemes research 2017 - 90% of large DC schemes but only 14% of small schemes feature admin on the board agenda quarterly)

Special projects (GMP, administrator switch, derisking) drive focus (RK qual research 2016)

What does this mean in practice? (2)

- Appropriate internal controls
  - SLAs, even with in-house administrators.
  - Processes to receive, check and review employer data
  - Processes around DPA and data breaches
    - More guidance coming from TPR
- Data review
  - Annually and on triggering events
  - Robust!
- Robust improvement plans
  - New TPR guidance

The Pensions Regulator

Appropriate internal controls

Private sector – SLAs more common in large schemes (87%) and rare (23%) in micro schemes

PS – TPAs (64%) vs in house (43%). Most FPS admin outsourced

Processes in place to receive, check and review employer data – FPS 76%

Private sector - The vast majority of schemes and their administrators are trained on DPA (more than 90%, rising to 99% for large schemes), and most have processes in place to ensure data breaches are reported to the administrator and then to the board (95% large, 81% small) DC research 2017

Data review

*-FPS **68%** in last 12 months; 2**0%** don't know; **39%** no issues identified*

-Private sector - Larger schemes identify more issues - 72% of large schemes found issues, 45% of medium and only 22% of small. DC research 2017

Robust improvement plans

FPS 2%, overall 18% (compares to c 50% DC schemes)

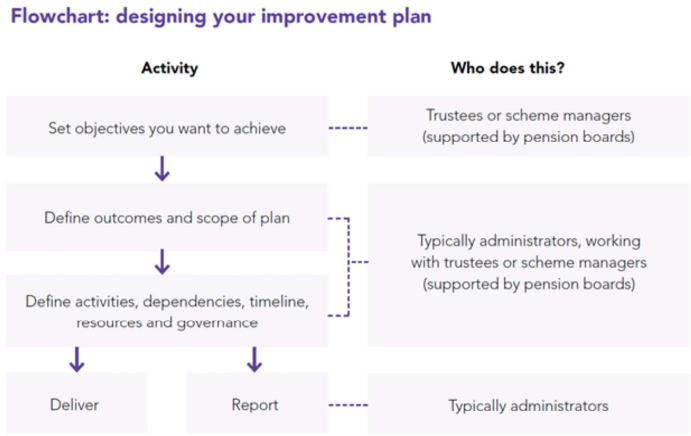
TPR activity

- Quick guide to record-keeping published in November 2017
- Quick guide to improvement plans published September 2017
- Record-keeping measures being introduced in scheme return 2018
  - New: common/key scheme-specific data
  - Clarity on how to measure data and what we mean by quality
- Assessing pension scheme landscape's cyber security
- Refreshed materials inc toolkit

The Pensions Regulator

Improving your data quick guide

- Aim to help design a plan or assess an existing one,



The Pensions Regulator

Objectives – your plan should set out the objectives you are aiming to achieve by improving your data.

E.g. Improving members' experiences by providing members with online access to their records; improving your ability to run scheme effectively by addressing data issues; preparing for transition to new admin system or new administrator

Outcomes - set out the outcomes to be achieved, including how they'll be measured and timescales

e.g. Fewer member complaints; more member comms issued accurately & on time; reduced administration costs; fewer assumptions in valuation data

Scope & prioritising – what data is included, what membership types are included, how far back improvement work will go. As a general rule you should prioritise data which will have the greatest impact.

Breakdown of activities your administrator will undertake for you as part of improvement plant - including issue to be addressed; methodology to be used, resource allocation, assumptions made, timescales & target dates, success criteria.

Dependencies

work impacting on your improvement work, where data is changed or same resources are used e.g. valuations, member communications, negotiating an administration contract

Timeframes & timelines

helps to identify hard deadlines and where additional resources may be required

Resourcing

impact of the work either being ‘business as usual’ administration or a separately managed project

Governance & reporting

roles & responsibilities, decision-makers, administrator reporting – how, to whom and when?

In summary

- Good data is critical to the running of your scheme
- GDPR is one of many drivers of good data management.
- Take action now: assess your data and put an improvement plan in place

The Pensions Regulator