Appendix 1

General Data Protection Regulations (GDPR)

Presented by James Ahlberg
Information Governance Manager

LPP
Local Pensions Partnership

What I will be covering…

- Background to the General Data Protection Regulation
- Why is it important?
- Key changes that will affect the LGPS
- First steps towards compliance
- Update on LPP's progress

LPP
Local Pensions Partnership

Background to General Data Protection Regulation (GDPR)

- What is it?
  - An EU regulation which will replace current EU Data Protection Directive 95/46/EC and the UK Data protection Act 1998
  - It provides a new legal framework setting out rules for processing personal data across the EU
  - Reinforces the existing law – Data Protection Act 1998 but:
    - Much more prescriptive
    - Higher penalties for non-compliance

- When does it come into force?
  - 25th of May 2018
  - Brexit to have little or no impact

LPP
Local Pensions Partnership

Why is it important?

Giant leap in penalties – up almost 4000%!

- Fines of up to greater of 4% annual worldwide turnover or €20 million for breaching key principles:
  - Data Security
  - Fair & Lawful processing
  - Transferring data outside the EU
  - Data subjects rights i.e. right of access, rectification, erasure

- Lower tier fines up to greater of 2% of annual worldwide turnover or €10 million for breaching lesser principles:
  - Failing to notify a data breach on time
  - Failing to have correct contract with service provider

LPP
Local Pensions Partnership

Why is it important?

Claims for compensation & other remedies

- Individuals can claim compensation for material and non-material damage i.e. Distress
- Not-for-profit bodies can bring representative actions on behalf of individuals
- New liability for data processors (pension administration service providers, IT providers etc) but data controllers (Administrating Authorities) remain primarily liable

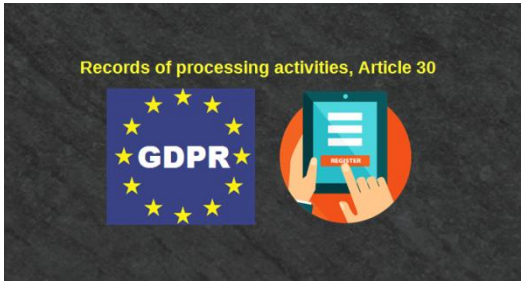
- Additional wide powers:
  - Investigative i.e. demand information/ audits
  - Obtain access to premises, equipment etc
  - Warnings, temporary/ permanent bans on data use, order suspension of data flows

LPP
Local Pensions Partnership

Key changes that will affect the LGPS

Data Mapping/ Records of processing activities (article 30)

- Name and contact details of controller and DPO
- Purpose
- Categories of data and data subjects
- Categories of recipients
- Transfers to third countries, and documentation of safeguards
- Where possible, time limits to erasure
- Where possible, description of security measures
- Make available to Supervisory Authority on request



LPP
Local Pensions Partnership

Key changes that will affect the LGPS

Data Protection Officer (Article 37-39)

- Mandatory because a public authority
- Potentially could be one DPO for several authorities
- Basis of appointment
  - Professional qualities
  - Expert knowledge of data protection law
  - Ability to perform required services
- Must be actively involved in all issues relating to personal data
- Must report directly to most senior management

LPP
Local Pensions Partnership

Key changes that will affect the LGPS

Enhanced Privacy Notices – more information in a shorter notice!

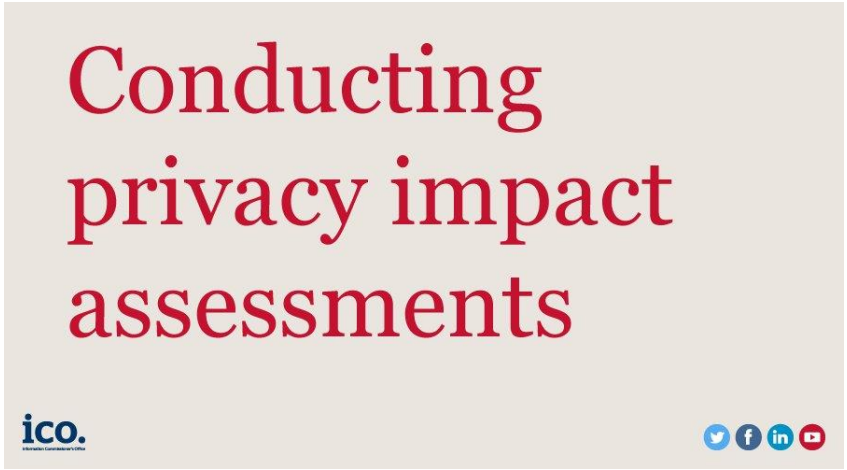
- All existing privacy notices need to be revised to include new mandatory information (Articles 14 & 14a)
- Must be concise and intelligible, so more information but shorter text!
- Solutions:
  - Layering - Short summary of key/unusual data uses, plus link to fuller privacy notice
  - Just in time notices i.e. when sign up to a new service
  - Privacy dashboards – meaningful choices about data uses
  - Videos or animations
- Stricter limits on use/effectiveness of consents

LPP
Local Pensions Partnership

Key changes that will affect the LGPS

Privacy Impact assessments? (Article 33)

- Required where "high risk" to rights and freedoms of individuals, including:
  - Systematic and extensive evaluation based on automated processing, including profiling, that significantly affects individuals; or
  - Large scale processing of sensitive personal data



LPP
Local Pensions Partnership

Key changes that will affect the LGPS

Privacy by Design and Default

- Requires right level of data protection to be embedded in life cycle of applications, taking account of
  - available technology
  - cost
  - risks

- To include data minimisation and pseudonymisation

- Default settings must ensure that only the specific personal data needed for the purpose is processed i.e. amount of data, extent of processing, period of storage and accessibility.

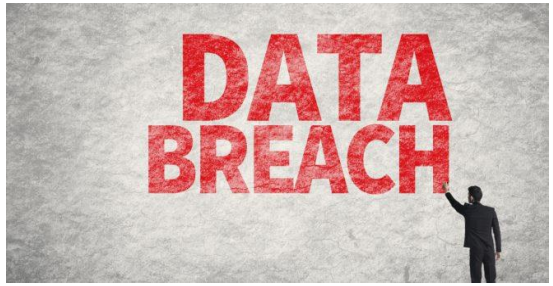
- Increased importance of limiting amount of data collected and what is shared

LPP
Local Pensions Partnership

Key changes that will affect the LGPS

Mandatory data breach notification – Robust data breach policy essential

- Must notify ICO of data breach unless unlikely to result in risk to individuals (i.e. some damage, or even loss of control of data)
- **Without undue delay** and where feasible within 72 hours after having become aware of the breach
  - Full details of the breach i.e. nature, categories and number of individuals affected, likely consequences and measures to address/mitigate the breach
- 72 hours = very short timescale – effective data breach handling procedure essential
- A *processor* shall notify the *controller* without undue delay
- A notification to the data subject **without undue delay** is also mandatory if breach likely to result in a high risk (not if encrypted so unintelligible)
- Controllers must document data breaches



LPP
Local Pensions Partnership

Key changes that will affect the LGPS

Service provider agreements – renegotiation & redrafting

- Expanded list of mandatory clauses to be included in every agreement that starts or continues after 25 May 2018

- For first time, direct obligations on processors, including
  - Security measures
  - Records of processing activities
  - Compliance on cross-border transfers
  - Co-operation with controller on compliance

- Big change in risk profile for processors
  - So likely to look to limit liability/seek indemnities

LPP
Local Pensions Partnership

Key changes that will affect the LGPS

And don't forget…

- Data Security – Will remain critically important
- Subject Access Requests – Will continue/increase in frequency
- Transfers Outside EEA – Will continue to need special terms/justifications
- Profiling/Automated Decision-making – Restrictions have been strengthened
- Right to be Forgotten - Expanded

LPP
Local Pensions Partnership

First Steps Towards Compliance

STEP 1 – Data Mapping & Gap Analysis

- Audit current position & identify major gaps in compliance
- Create/update records of personal data processed
- Develop & implement a compliance plan

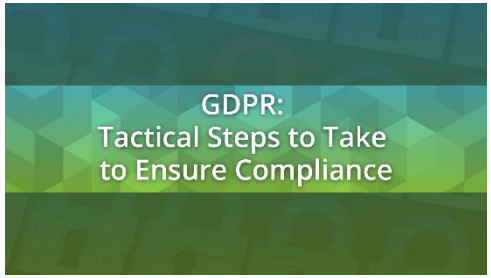
STEP 2 – Data Privacy Officer

- Agree appropriate structure & roles for DPO(s)
- Develop job specification
- Recruit/appoint DPO(s)

STEP 3 - Data Protection Policies & Procedures

- Identify & review existing policies/procedures
- Update and add to these as required

LPP
Local Pensions Partnership



First Steps Towards Compliance

STEP 4 – Review data security & breach handling processes

- Review and update data security systems, processes & procedures
- Prepare and/or update data breach response plans

STEP 5 – Service Agreements

- Identify and prioritise existing agreements for review/renegotiation
- Revise standard templates to include new mandatory provisions

STEP 6 - Privacy Notices

- Update to insert mandatory content
- Consider layering notices

STEP 7 - Check you can 'demonstrate' compliance

LPP
Local Pensions Partnership

Update on LPP's progress

Step	LPP Progress
1	• High level & detailed gap analysis completed • Data mapping for admin business completed, other areas of the business ongoing
2	• DPO in place and a new Information Governance Manager appointed to head up GDPR implementation
3	• All policies and procedures identified and in the process of being updated
4	• A new process and system to report data breaches has been implemented • A detailed staff training plan for all staff is underway for roll out in March
5	• All service agreements have been identified and are in the process of being reviewed to ensure compliance by May 25th • Legal have drafted the supplemental agreement which is currently being reviewed
6	• LPP's Fair Processing Notice (FPN) is in draft format ready for review • Other privacy notices for the business are under review
7	• All decisions made are being recorded so LPP can demonstrate compliance to the ICO in case of audit or we have a data breach

LPP
Local Pensions Partnership

Any questions?

Source information for presentation gathered from Information Commissioners Office, Squires Patton Boggs & Dilys Jones Associates Ltd.

LPP
Local Pensions Partnership