West Yorkshire Pension Fund

General Data Protection Regulation (GDPR)

What is GDPR?

The General Data Protection Regulation (Regulation (EU) 2016/679) was devised by European Parliament, Council and Commission to strengthen and unify how we use and protect data for individuals situated within the European Union.

GDPR is replacing the Data Protection Act 1998.

Must be fully implemented by 25 May 2018.

BREXIT – does GDPR still apply?

Will come into effect before Brexit is completed and the UK Government is seeking to transpose existing EU legislation in to UK as part of Brexit.

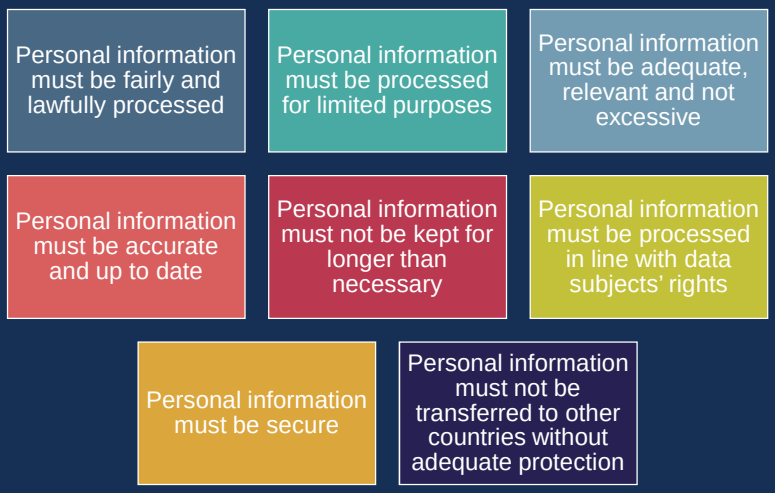
Any individual within an EU country is to be provided data security in line with the GDPR.

Data Protection Roles

- **Information commissioner:** person who has the power to enforce the Act
- **Data controller:** person or organisation that collects and keeps data about people
- **Data processor:** person or organisation that processes data on behalf of the data controller
- **Data subject:** person who has data about them stored outside their direct control

GDPR applies to Data Processors as well as Data Controllers with effect 25 May 2018.

Data Protection Principles



An Individual's Rights - GDPR

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.

Changes under GDPR

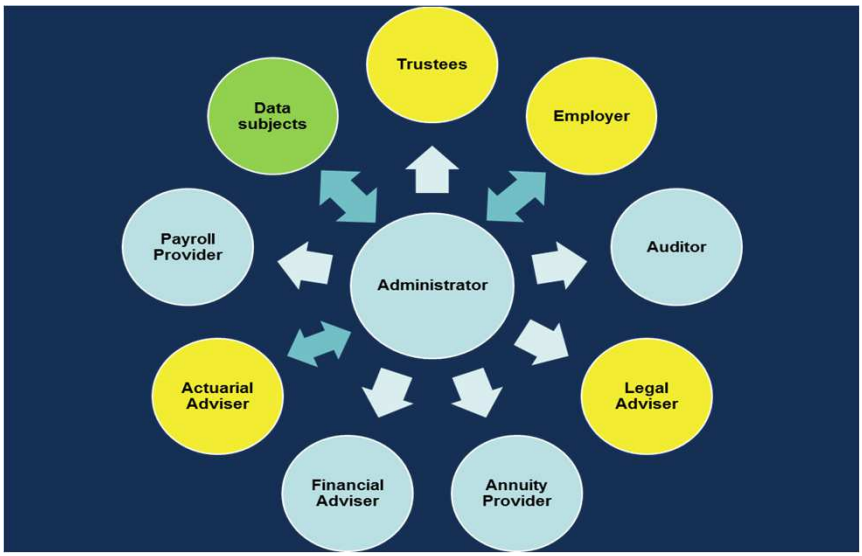
1. Breach notifications
   72 hours to report from becoming aware of a breach
2. Right to access (Data Subject Access Requests – SAR's)
   Timescale changed from 40 calendar days and optional £10 fee to 30 calendar days and free of charge
3. Right to be forgotten (aka data erasure)
   Individuals can ask for any or all of their information to be removed from all systems
4. Data portability
   Individual's data must be able to be transferred in a "commonly used" and machine readable format
5. Compliance by design
   Inclusion of data protection from the onset of designing systems, policies and procedures – including PIA's (privacy impact assessments)
6. Data Protection Officer
   DPO is a mandatory only for controllers and processors whose core activities consist of processing and monitoring on a large scale or of special categories of data or data relating to criminal convictions and offences.

Changes under GDPR

1. Privacy Impact Assessments
   For each process and each change of process, must be published
2. Privacy Statement
   Published on the website confirming adherence to GDPR and how we comply
3. Fair processing notice
   Why we hold the data and what we use it for (including sharing with third parties)
4. Consent
   Must be proactively given, not passive
5. Children's data
   Where we hold Children's data all of the above information must be written in a way for them to understand.
6. Overseas members
   May be subject to a different version of GDPR depending on individual member state adoption.

Sanctions for non-compliance

- a warning in writing in cases of first and non-intentional non-compliance
- regular periodic data protection audits
- a fine up to 20,000,000 EUR or up to 4% of the annual worldwide turnover of the preceding financial year, whichever is greater



West Yorkshire Pension Fund | Lincolnshire Pension Fund

PO Box 67 • Bradford • BD1 1UP
www.wypf.org.uk

lgps

Where is data stored?

Laptops/ devices

Spreadsheets

Paper records

Meeting papers

USB sticks

Microfiche

Database

Cloud based storage

Emails

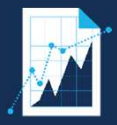
Who is processing our data?

What personal data is held?

- Names
- ID numbers
- Gender
- Medical records
- Dates of birth
- Criminal records
- Contact details
- Salaries
- Pension payments
- Marital status
- Dependants' details
- Service dates
- Employment history
- Bank details
- Benefits
- Contributions

What is data being used for?

Scheme administration



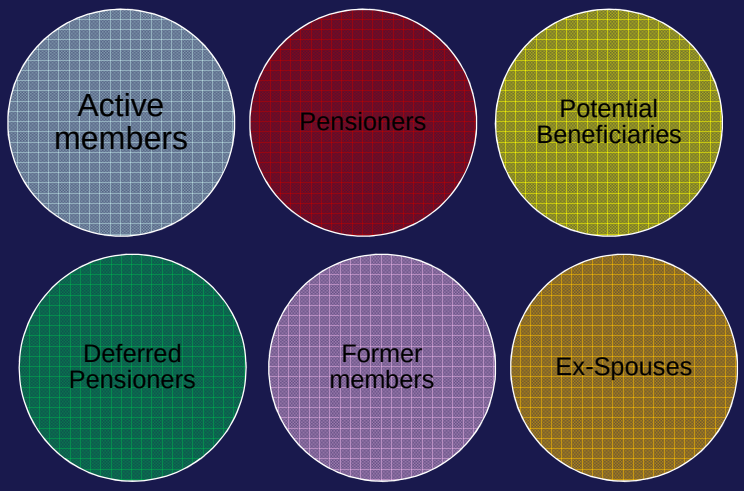
Actuarial valuations

Preparing accounts

Providing legal advice

Exercising discretionary powers

Who are the data subjects?



Who is data shared with and how?

DOCUMENT ALL DATA FLOWS

- *How is data stored?*
- *Is it secure?*
- *Is data shared outside the EU?*
- *Are there any alternatives?*

How long is the data kept?

- *How long should you keep data?*
- *What about former members?*
- *How long are our processors keeping data?*
- *How is data destroyed?*
- *Ask to see each party's policy on data destruction*

RECORD OF PROCESSING ACTIVITIES

Processing details

Who holds the data?	*Processor or controller?*	*What personal data do they hold?*	*Why are they using the data?*	*Who are the data subjects?*	*Will the data be shared with any third parties?*	*Is data transferred outside EEA?*	*How long is data kept?*	*How is the data secured?*
Trustees	Joint Controller		Scheme administration		Administrators	No	Lifetime of scheme	
Administrators	Processor	Names, DOB, gender, contact details, service dates, salaries, benefits	Scheme administration	Active members, deferred members, pensioners, former members, potential beneficiaries, ex-spouses	Trustees, Actuary, Legal Advisers, IFAs, etc	No	Lifetime of scheme	
		Special categories of data - medical records, sexual orientation	Ill-health retirements, nomination forms			No	x years after event	
Employer	Controller in common				Administrators	No		

Is data secure?

- Pseudonymisation/encryption
- Is security regularly tested?
- How quickly can data be restored
- Relevant accreditations
- Ask to see each processors security policy

Summary

1. *Coordinate data mapping and ongoing requirement for records of processing activities*
2. *Keep in mind all the locations data is stored*
3. *Consider each processor in turn*
4. *Don't forget former advisers and former trustees*
5. *Make sure your data is current*
6. *Keep it simple and focussed but legal*
7. *Don't forget data on trustees/advisers themselves*
8. *Don't forget sub-processor*
9. *Don't be afraid to keep data long term as long as you can justify it.*
10. *Document policies via links in spreadsheet*

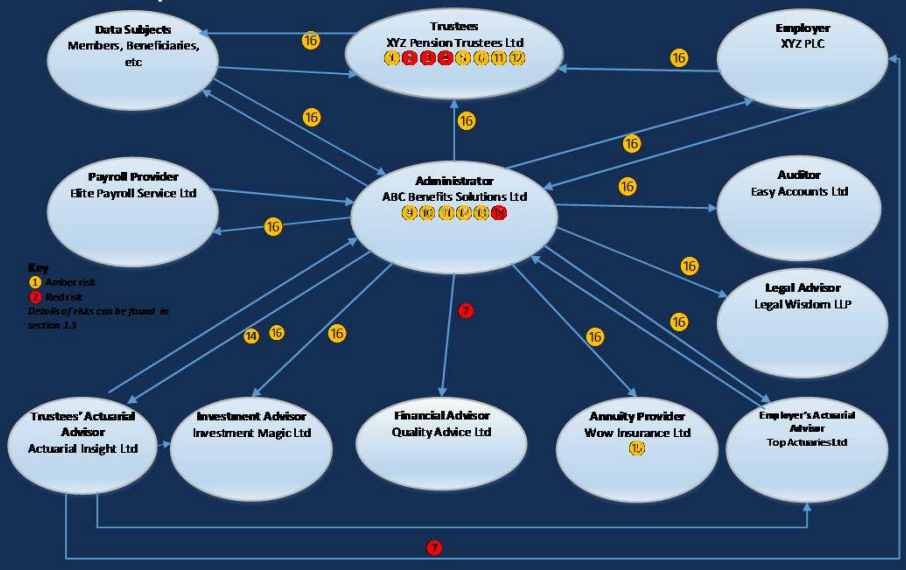
Summary of tips

itm
Solution delivered...

1 / *Coordinate data mapping and ongoing requirement for records of processing activities*
2 / *Keep in mind all the locations data is stored*
3 / *Consider each processor in turn*
4 / *Don't forget former advisers and former trustees*
5 / *Make sure your data is current*
6 / *Keep it simple and focussed but legal*
7 / *Don't forget data on trustees/advisers themselves*
8 / *Don't forget sub-processor*
9 / *Don't be afraid to keep data long term as long as you can justify it*
10 / *Document policies via links in spreadsheet*

Data / Systems / Consultancy

Data map with risks



Questions

West Yorkshire Pension Fund | Lincolnshire Pension Fund

PO Box 67 • Bradford • BD1 1UP
www.wypf.org.uk

lgps