Quattro Pensions
CONSULTING ACTUARIES

# news bulletin

Prospect House,
Fishing Line Road,
Redditch,
Worcestershire B97 6EW
**Tel: 01527 598688**
www.quattropensions.com

## Get ready for GDPR

The Government has confirmed that, despite Brexit, the European Union's General Data Protection Regulation (GDPR) will come into force in the UK on 25 May 2018 and contains significant changes to data protection requirements. **The GDPR will apply to all data controllers and data processors of pension schemes so it is important that trustees (and their advisers) are aware of and are prepared for the upcoming changes.**

Whilst the principles remain similar to those in the Data Protection Act (DPA), GDPR adds much more detail at certain points and introduces a new **accountability requirement** requiring data controllers and processors to be able to demonstrate compliance.

The requirements of GDPR apply to 'personal data' and 'sensitive personal data', the definitions of which have been widened. The inclusion of online identifiers, such as IP address, within the definition of 'personal data' shows how the legislation has been updated to fit in with the digital age.

Under GDPR, trustees must have a lawful basis for processing members' personal data. **This should be documented and an explanation of it should be provided in the privacy notice.** Where consent is used as the lawful basis for processing data trustees should note that GDPR gives members stronger rights, including the right to have their data deleted.

The fines for non-compliance under GDPR have been significantly increased and could be up to €20 million (or 4% of global turnover if greater). Organisations have 72 hours from becoming aware of a breach to reporting it to the Information Commissioner's Office (ICO). Firms that regularly store and monitor large amounts of data will be required to appoint a Data Protection Officer (DPO) who will be responsible for data protection compliance.

One of the areas where fines for non-compliance have significantly increased is the transfer of personal data outside of the European Economic Area (EEA). Trustees should ensure they have the appropriate mechanisms in place to comply with GDPR.

Data protection by design is to become a legal requirement (rather than just good practice) meaning that GDPR compliance should be integrated into all data processing activities from the outset. GDPR also requires data protection impact assessments (DPIAs) to be conducted in situations where data processing is likely to result in high risk to individuals.

GDPR increases the standards for consent from individuals, noting that it must be specific, granular, clear, prominent, opt-in, well documented and easily withdrawn. Trustees should review their mechanisms for seeking, recording and managing consent.

Data protection should be included on the agenda for all trustee meetings well before May 2018. **Contracts with administrators and others are likely to require change.**

As data controllers, trustees should have a plan in place to make sure they are ready for the changes coming into effect on 25 May 2018, which should include:

### Data Mapping

A detailed data mapping exercise should be carried out to identify all data processing activities and to establish if you have a lawful basis for processing data under the new GDPR requirements.

### Review Scheme Governance Documents

Update internal policies and procedures, including the risk register, to ensure they are compliant with GDPR.

### Contracts & Service Agreements

Review contracts and service agreements with third party advisers to ensure they are compliant with GDPR and that they clarify the allocation of responsibility if involved in a breach.

### Individuals' Rights

Ensure adequate procedures are in place to deal with the new and enhanced rights for individuals.

### Member Communications

Review all member communications, including privacy notices, for compliance with GDPR. Identify any new pieces of information you are required to provide to members.

Where the above actions are delegated to the scheme's administrator (acting as data processor on behalf of the trustees), trustees should obtain confirmation that the administrator will be carrying them out.

Trustees should consider obtaining legal advice throughout.

Please speak to your usual Quattro contact to find out more about the proposed changes and how they may affect you.

August 2017