Spotlight on Pensions
PRESENTS
Le Grand View
SEPTEMBER 2017

GDPR – Will you be ready?

The data protection rules applicable to occupational pension schemes in the UK have been clearly established since the Data Protection Act 1998 came into force. But now there's a New Kid on the Block, courtesy of the EU – GDPR, the **General Data Protection Regulation.**

Increases in the value of personal data and the lengths to which some will go to obtain and exploit it mean that the original regulations are no longer tough enough.

Many trustees currently fail to realise the value of even basic member data to fraudsters, and therefore the attractiveness of the scheme as a target, particularly through cyber crime. GDPR seeks to protect data from outside threats while ensuring that it is not unreasonably exploited by those who hold it legitimately.

This new regulation applies across the whole of the EU from 25 May 2018 without the need for a member state to incorporate it directly into its own domestic legislation. That means that UK organisations, including pension schemes, will have to comply. And even post-Brexit, the possible need to handle data from other countries in the EEA will mean that schemes cannot take the risk of non-compliance.

The new regulations are much tougher than the old, meaning that organisations will have to review their processes, procedures and records by the 25 May deadline. And if you were thinking of ignoring it in the hope that it will go away, the advice is: Don't. Breaches can attract a penalty of up to 4% of an organisation's worldwide annual turnover, or €20 million, whichever is higher.

This new regulation applies across the whole of the EU from 25 May 2018 without the need for a member state to incorporate it directly into its own domestic legislation.

Building on the old

So what's different (apart from those awesome penalties)? What new things will trustees have to do to be compliant? First, let's look at what's continuing from the current regime.

The eight core data protection principles under the 1998 Act will essentially remain. In summary, they require that personal data is:

(i) fairly and lawfully processed

(ii) for limited purposes (i.e. obtained for one or more specific purpose(s) and not processed in any manner incompatible with that purpose)

(iii) adequate, relevant and not excessive (i.e. individual items held are not excessive for the purpose required)

(iv) accurate (e.g. also kept up to date)

(v) not kept for longer than necessary (e.g. if not needed again, destroyed)

(vi) processed in accordance with the data subject's rights

(vii) secure (e.g. protected against unlawful access, accidental loss or damage etc.), and

(viii) not transferred to countries outside the European Economic Area without adequate protection.

GDPR builds on that base by bringing the principles more up to date and by introducing additional requirements.

New requirements

Key changes under GDPR include:

(a) ***new data processor obligations*** – data processors will now have direct obligations similar to those of data controllers, and will require prior consent from the data controller before using sub-processors

(b) ***transparency*** – more openness about how data are handled and simpler, clearer information

(c) ***explicit consent*** – where consent is required it has to be given explicitly and freely, and be informed consent

(d) ***notification by organisations within 72 hours*** – if data are accidentally or unlawfully destroyed, lost, altered, accessed or disclosed to unauthorised persons (i.e. data breaches)

(e) ***increased responsibility and accountability*** – through data protection risk assessments and the appointment of expert data protection officers

(f) ***a right to be forgotten*** – and the right to access copies of personal data free of charge

(g) ***data protection impact assessments*** – on the impact on members, are required when introducing new technologies.

What pension trustees need to do

Most schemes will need to introduce some new measures and change some working practices. Key points include:

- Accommodating the fact that their data processors such as administrators and other third parties will have similar obligations to those already imposed on trustees, as data controllers. The greater obligations should be reflected in service agreements.
- Making more detailed disclosure to scheme beneficiaries, including how their data are used by the scheme. Permission to use beneficiaries' data will need to be actively sought.
- Processes and procedures to identify, investigate and, if necessary, report breaches within the new 72 hour deadline will be needed.
- At present it is not clear whether schemes will have to appoint a data protection officer, but trustees should seek legal advice on their particular situation.
- Impact assessments should become a standard part of any assessment undertaken on the introduction of new technologies.

Most schemes will need to introduce some new measures and change some working practices.

Action required

The scope of the required review and likely changes necessary to comply with GDPR mean that trustees who have not yet started the process have an uphill battle to become fully compliant by next May. Given the complexity of the likely changes and the importance of getting them right, most trustees will require legal advice, adding to the time needed. Trustees will also find it useful to look at the Information Commissioner's website: **https://ico.org.uk/for-organisations/data-protection-reform**.

One further key requirement arising out of the new regulations will be the need to keep a close watch and strict control over compliance. That points to a beefed-up section in the risk register, with a standing agenda item to review at every trustee meeting. Arguably, this should be trustees' first action, to ensure that the scheme is fully compliant by the appointed date.

Pendragon
Wilmington Risk & Compliance