Trustees - are you ready for the GDPR?

Baker McKenzie considers the preparatory work required by trustees before the GDPR comes into effect in May 2018

The EU General Data Protection Regulation (GDPR) comes into effect on 25 May 2018 and will significantly change the data protection regime in EU countries. In the UK, the GDPR will also be supplemented by a new Data Protection Bill, which is currently before Parliament and will ultimately replace the current Data Protection Act.

The GDPR will apply to all personal information collected and processed by trustees, employers, scheme administrators and third-party providers. The UK data protection regulator (the ICO) will be able to impose fines of up to 4 per cent of annual worldwide turnover or €20 million (whichever is higher) for GDPR breaches on 'undertakings'. It is currently unclear how the concepts of 'undertaking' or 'worldwide turnover' apply to an occupational pension scheme; however, there is clearly potential for fines to be significant.

All data controllers, including trustees, will be required to comply with the GDPR from May 2018. Preparing for this can be daunting, but we outline below five key areas for trustees (as data controllers) to focus on over the next five months.

What should you be doing to prepare?

• Consider legal grounds for processing scheme data

The GDPR will require trustees to assess and document the legal grounds on which they process personal data (such as consent, legitimate interest, or performance of contractual obligations). Trustees should therefore consider which ground(s) they rely on whenever processing member or beneficiary data.

Which ground is most appropriate is context dependent and should be analysed on a case-by-case basis. However, trustees may often be able to justify processing data based on a legitimate interest, provided this is balanced against individuals' rights. Where trustees rely on a legitimate interest, they should document the ways in which they ensure this 'balancing test' is met.

Trustees may historically have relied on consent to process certain data. However, the GDPR imposes stricter conditions on relying on the ground of consent and allows individuals to withdraw consent at any time. Trustees may therefore wish to reassess their options and consider whether other grounds may be available.

• Review methods of obtaining consent

If relying on consent as a legal ground for processing, trustees should review the ways in which consent is given. Under the GDPR, valid consent will require clear affirmative action; silence, inactivity or pre-ticked boxes are insufficient. For sensitive data, such as health information, 'explicit' consent is required; this likely means the consent will need to be expressly confirmed in words.

Trustees relying on consent should be able to demonstrate that they have obtained valid consent from all members and beneficiaries and that they have kept accurate record records of the same. Keeping clear records of any consents obtained will be key.

• Update privacy notices

Trustees will need to issue updated GDPR-compliant privacy notices to members and beneficiaries. Articles 13 and 14 of the GDPR include detailed requirements on the information these notices must contain. For example, trustees must provide members with information about their rights over their personal data, the legal basis and purposes for which that data is processed and details of any third parties receiving their data.

• Review and update agreements with third parties

Trustees should ensure that contracts with third-party service providers (such as administrators or actuaries) are updated to comply with the GDPR. In particular, Article 28 of the GDPR contains detailed requirements on the provisions that organisations must include in contracts with third parties processing data on their behalf. Current data protection clauses currently in trustees' contracts with service providers will almost certainly require updating.

• Demonstrate compliance (accountability)

Accountability (the principle that controllers must be able to demonstrate compliance) is a central concept in the GDPR. Trustees should ensure they can demonstrate accountability by providing, and documenting, staff training on GDPR, implementing internal privacy policies, maintaining accurate records of processing activities and carrying out impact assessments to assess data protection risks.

Written by Kate Atkinson, senior associate, Joanna de Fonseka, associate and Lauren Williams, associate, Baker McKenzie