# General data protection regulation

**Matthew Swynnerton looks at the implications for trustees of new data protection laws that come into force next year**

As data controllers, trustees of occupational pension schemes will need to ensure that they are ready to comply with a new EU General Data Protection Regulation (GDPR), which comes into force on 25 May 2018 and will apply in the UK without the need for implementing national legislation. Whilst many of the main concepts and principles of the GDPR are similar to those in the current data protection legislation, there are also some significant differences.

In this article we highlight some of the key action points that trustees will need to consider as part of their preparations. There may only be one or two full trustee meetings scheduled to take place before the GDPR comes into force and therefore trustees should consider whether to establish a GDPR sub-committee to deal with this issue in between trustee board meetings.

• Trustees should complete a data mapping exercise to assess what data the scheme holds, how it was obtained, why it is held, and who it is shared with. In addition, trustees should contact administrators, advisers and any other third parties who process data for them to ask what steps the data processors are taking to ensure compliance with the GDPR.

• Trustees will need to ensure that there is a lawful basis for each processing activity. The potential lawful bases for processing personal data under the GDPR include bases relating to the legal obligations of the trustees and legitimate interests pursued by the trustees. Special categories of personal data (such as data concerning health) can only be processed if one of a list of conditions is met, which include that the data subject has given explicit consent. The GDPR sets a higher standard for consent than the current legislation, including that an indication of consent must be unambiguous and a positive indication of agreement and individuals will also have the right to withdraw consent. If consent is used as the basis for any processing, it must be ensured that the way the trustees obtain and record consent meets the higher standards in the GDPR.

• The information that has to be provided to data subjects about the processing of their data is more extensive under the GDPR than the current legislation, and the GDPR also states that the information must be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language. Trustees will therefore need to review the privacy notices for their scheme and update them where necessary.

• The GDPR makes more extensive provision about the content of contracts between controllers and processors. Trustees will therefore need to review contracts with their data processors, such as administrators, and ensure that any necessary amendments are negotiated, agreed and in place by 25 May.

• The GDPR includes a new principle of accountability, which requires the data controller to be able to demonstrate compliance with the principles relating to the processing of personal data. It also requires data controllers to maintain records of processing activities. Trustees will therefore need to ensure that appropriate records and policies are in place to meet these requirements.

• The GDPR introduces duties to notify the relevant supervisory authority (which in the UK is the Information Commissioner's Office) within 72 hours of becoming aware of a personal data breach if the breach is likely to result in a risk to the rights and freedoms of individuals. Trustees will need to ensure that they have policies and arrangements with administrators in place so that they can comply with this obligation.

With less than six months to go until the GDPR is in force: trustees who have already started their preparations should check that they are on track with their project plans and that their plans cover all the necessary activities; and trustees who have not yet started to look at this issue should take action now as time is running out. There is a lot for trustees to do and therefore steps to ensure compliance with the GDPR are likely to feature heavily in all trustees' work plans over the next few months.

**Written by Matthew Swynnerton, partner in the pensions practice, DLA Piper**