Sackers

GDPR: countdown to 25 May 2018

Alert | 16 January 2018

Introduction

On 25 May this year, new data protection requirements will come into force aimed at creating a regulatory regime fit for the digital age. Much of the General Data Protection Regulation (GDPR) will feel familiar, as the new rules build on existing data protection provisions, but some important changes will be introduced.

By now, trustees and employers should be well on their way to understanding their responsibilities under the GDPR, and ensuring that updated processes and procedures in respect of their pension arrangements are in place.

Key points

- The GDPR will introduce new contractual obligations, increase the information that needs to be given to individuals, and enhance reporting obligations in the event of a breach.
- A new Data Protection Bill is currently undergoing scrutiny in the House of Lords. With a view to giving the UK "one of the most robust, yet dynamic" sets of data laws in the world, the Bill is designed, among other things, to replace the UK's existing Data Protection Act and bring provisions of the GDPR into UK legislation, subject to certain amendments.
- Non-compliance with the new data protection requirements will be met with heavier sanctions, with maximum penalties of up to €20,000,000 (£17,000,000) or 4% of an organisation's global turnover. While it is not yet clear how the latter penalty will apply to bodies such as pension scheme trustee boards which do not have annual turnover, the increase in fines from £500,000 currently is clearly significant.

1 Audit your personal data

Under the GDPR, "personal data" is any information (whether opinion or facts) relating to an identified or identifiable living individual. An individual can be identified or identifiable, directly or indirectly, by reference to an identification number or to one or more factors specific to his/her identity. The fact that information is publicly available, such as on social networks, does not stop data protection legislation applying to it.

In a pensions context, personal data may be held on both current and former members, as well as their dependants and beneficiaries (both actual and potential), and will include names, postal addresses, email addresses, dates of birth, national insurance numbers, bank account and salary details, length of

pensionable service and pension benefits.

As the ultimate responsibility for member data rests with a pension scheme's trustees, the trustees are "data controllers" for the purposes of the GDPR. As such, they are responsible for ensuring that any personal data is processed in a way that complies with relevant requirements. If not, trustees potentially risk enforcement action (including prosecution) by the ICO and compensation claims from individuals.

Trustees therefore need to make sure they know what personal data they hold, why they hold it, who else has access to it, how long it has been held, and whether it is still needed. Our checklist on assessing pension scheme data can help you assess what personal data you hold and why.

2 What grounds do you have for processing personal data?

For the processing of non-sensitive personal data to be lawful, at least one of six conditions must be met. Trustees therefore need to decide the basis (or legal grounds) on which they process scheme member personal data. Grounds which are likely to apply to pension schemes include:

- the processing being necessary for legitimate interests pursued by the data controller or a third party (such as the effective running of the pension scheme by the trustees and scheme administrator)
- compliance with legal obligations to which the trustees (as data controllers) are subject
- the processing being necessary for the performance of a contract (generally more relevant to employers and personal pensions)
- the member having given their consent to the processing of their personal data for one or more specific purposes.

Consent will generally be required where sensitive personal data (such as data relating to a member's health, sex life or sexual orientation) is being processed. Where consent is used as a basis for processing members' personal data, the procedures for obtaining consent should be reviewed and updated.

3 Update your contracts

The GDPR sets out specific requirements on how relationships should be documented where personal data is being shared between certain parties. The purposes for which personal data is collected and used, and who is in the driving seat when it comes to deciding that, will be essential in determining the contract wording required.

There are no specific requirements in the GDPR on documenting data sharing between separate data controllers (each data controller being independently responsible for compliance). However, entering into an agreement covering some essentials is advisable, such as the receiving data controller undertaking to abide by its obligations under the GDPR, and limiting the use and onward transmission of the personal data.

Trustees will need to have a binding contract in place with any data processor whose services they engage, such as the scheme administrator, setting out the subject matter and duration of the processing, the nature and purpose of the processing, the types of personal data involved, and the categories of individuals on whom it is held.

Our checklist on governance and contractual requirements explains in more detail the steps trustees should be taking to document data sharing arrangements (see Parts 4 and 5).

4 Communicate with members

The GDPR will introduce additional requirements affecting the provision of information to members. Trustees will need to issue revised information notices (also known as privacy statements), and it is likely that existing information will need to be updated.

Among other things, privacy statements will need to include: the identity of the data controller (generally, the trustees) and their contact details, the purpose(s) for which personal data is processed and details of the legal basis relied on. It should also explain who will receive members' personal data, how long it will be kept, information about transfers of data outside of the EEA (and where details of the safeguards relied on can be obtained), and relevant individuals' rights (see further below). Members will also need to be given notice of the right to complain to the ICO.

Where trustees are joint data controllers, for example with the scheme actuary, the trustees may wish to prepare a joint privacy notice.

5 Do members know their rights?

Trustees need to tell members how their personal data is processed and ensure that members are fully aware of their rights in relation to the personal data that is held. These include rights:

- to be informed as to what personal data is held, as well as who holds it and how it is processed
- for members to access their personal data
- to have personal data rectified if it is inaccurate or incomplete
- to request the deletion or removal of personal data where there is no compelling reason for its continued processing (the "right to be forgotten")
- to restrict processing, for example, where a member contests the accuracy of the personal data held
- to object to processing on grounds relating to a member's particular situation.

Trustees should ensure that their processes (and those of their advisers) are ready to deal with any such requests from members.

6 Review your policy

As data controllers, trustees will need to implement appropriate measures to comply with the GDPR. This includes protecting individuals' rights, reducing the risk of data breaches occurring, managing any breaches that do occur, and demonstrating that they are taking GDPR compliance seriously. The trustees' data protection policy will be the main document for recording how they look after personal data in relation to their scheme, reflecting key decisions taken and procedures put in place to meet GDPR requirements.

The content and structure of data protection policies will vary from scheme to scheme but should aim to cover certain points as a minimum in line with record keeping requirements under the GDPR. For trustees, a key aspect of their policy will be to set out details of the procedures they put in place to safeguard the security of personal data, including cyber security, and the requirements placed on data processors acting on the trustees' behalf. Details of the information to be given to members in the trustees' privacy notice (see 5 above) should also be set out.

The policy should also cover the process for keeping these components under review, and include a procedure for dealing with and recording any breaches of the policy / GDPR requirements generally. Our checklist on governance and contractual requirements explains in more detail what trustee data protection policies should include (see Part 3).

7 Do you need a Data Protection Officer?

Both data controllers and processors will need to appoint a data protection officer ("DPO") in certain circumstances, for example, where their "core activities" involve "regular and systematic monitoring of data subjects on a large scale", or consist of "large scale" processing of sensitive personal data.

Whilst it is unlikely that occupational pension schemes trustees will need to appoint a DPO, all schemes should assess whether they need one with input from their legal advisers and document their conclusions.

8 Understand your role

Key to GDPR compliance is ensuring that you understand what is required under the new rules. Available from our website are a number of Alerts and a series of checklists setting out key questions and actions for occupational pension scheme trustees, to help you meet the new requirements.

We can also offer bespoke training to help you get up to speed.

9 Be ready to demonstrate compliance

A new principle of accountability requires data controllers to be responsible for, and able to demonstrate compliance with, the data protection principles. Steps that trustees can take to fulfil their obligations include:

- undertaking appropriate training and checking that their advisers have also done so
- carrying out a data audit (described in section 1 above)
- reviewing internal policies and agreements with third parties (such as administration agreements)
- documenting decisions as to how personal data is processed, including the purpose(s) for which it is processed, and how the GDPR principles will be met in the scheme's data protection policy.

10 How well protected are you?

Trustees should check what protections may be available to them in the event of any regulatory fines from the ICO or compensation claims from individuals arising from a data protection breach. For example, do they have insurance cover in place which might protect them in these circumstances?

As not all trustee insurance policies will cover such fines or compensation claims, it is important that trustees check with their legal advisers the extent of any cover, and whether any other trustee protections may apply. Trustees should also check the extent to which they are covered in the event of cyber security breaches.

Next steps

We can help trustees prepare for the GDPR in a number of ways, including reviewing existing or new contracts, updating your data protection policy, reviewing procedures, and drafting member communications.

For assistance with any of these, or any other GDPR query you may have, please speak to your usual Sackers contact.

Sacker & Partners LLP
20 Gresham Street
London EC2V 7JE
T +44 (0)20 7329 6699
E enquiries@sackers.com
www.sackers.com