Sackers

GDPR – a new era dawns

Alert | 25 May 2018

Introduction

The GDPR is in force from today, 25 May 2018. Aimed at creating a regulatory regime fit for the digital age, the GDPR builds on existing data protection provisions, many of which will feel familiar. However, there are a number of important changes that trustees and employers need to be aware of.

Key points

- 25 May 2018 marks the dawn of a new era for the protection of personal data. Trustees have been working hard to get ready, and will continue to adjust as the new requirements bed down. Compliance is an ongoing process, not a one-off exercise.
- The GDPR introduces new contractual obligations. It also adds to the information which needs to be given to individuals, and increases data breach reporting obligations.
- A new Data Protection Act aims to give the UK "one of the most robust, yet dynamic" sets of data laws in the world. The Act replaces the earlier DPA, bringing the provisions of the GDPR directly into UK legislation.
- To help trustees and others prepare, we have produced a series of Alerts and checklists on various elements of the new requirements. These are available from the data protection area of our website.

Background

In the pensions context, personal data may be held on both current and former members, as well as their dependants and beneficiaries (both actual and potential). It can include, among other things, 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 scheme personal data rests with them, 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. Failure to do so risks enforcement action (including prosecution) by the ICO and compensation claims from individuals.

Key steps towards compliance

Audit your data

For most trustees, the starting point has been a personal data audit or mapping exercise, to identify what personal data they hold, why they are holding 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 here.

Determine grounds for processing

Trustees must determine what legal grounds they have for processing scheme personal data. Usually, there will be more than one. Common grounds for pension schemes include the processing being necessary for legitimate interests pursued by the trustees, compliance with legal obligations (such as pensions and tax law), the processing being necessary for the performance of a contract (generally more relevant to employers and personal pensions), or members having given their consent to the processing of their personal data for one or more specific purposes (we expect consent to be used mainly where trustees are processing sensitive personal data).

Where consent is used as a basis for processing members' personal data, trustees' procedures for obtaining consent should be reviewed and updated.

Update your contracts

The GDPR sets out specific requirements on how agreements should be documented where personal data is 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, are essential in determining the contract wording required.

There are no specific requirements on documenting data sharing between separate data controllers where each is independently responsible for compliance. But 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 must have a binding contract in place with any data processor whose services they engage, such as the scheme administrator (including, we suggest, in-house administration or scheme secretarial services). 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).

Data protection policy

Trustees need to have appropriate measures in place to comply with the GDPR. These include protecting individuals' rights, reducing the risk of personal 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.

The content and structure of the data protection policy 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. Trustees may also wish to have separate policies or guidelines dealing with discrete aspects of data protection, such as their processes for safeguarding the security of personal data, managing personal data breaches and individuals' rights, and a policy on data retention.

Our checklist on governance and contractual requirements explains in more detail what trustee data protection policies should include (see part 3).

Communicate with members

The GDPR introduces new requirements affecting the provision of information to members. If they have not already done so, it would be sensible for trustees to issue revised information notices (also known as privacy statements). Part 2 of our checklist on individuals' rights under the GDPR explains what these notices need to contain.

As the GDPR requires a wide range of detailed information to be provided, a practical approach being adopted by trustees (as suggested by the ICO), is to provide information in "layers", signposting key privacy information immediately, whilst making more detailed information available elsewhere for those that want it (such as on the scheme's website).

Members' other rights

Trustees should ensure that members are fully aware of their data protection rights, including the right to access their personal data. Parts 3 to 5 of our checklist on individuals' rights under the GDPR set out key questions and actions for trustees in this area. Trustees should ensure that their processes (and those of their advisers) can cope with any such requests from members.

Demonstrate compliance

A new principle of accountability means that data controllers are responsible for, and must be able to demonstrate compliance with, the data protection principles. In addition to the steps outlined in this Alert, trustees can also demonstrate compliance by undertaking appropriate training.

Protections for trustees

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 consider the extent to which they are covered in the event of cyber security breaches.

Recent developments

Obtaining consent

The ICO's final detailed guidance on consent was published in May 2018. Aimed at helping data controllers to manage consents under the GDPR, it provides guidance on when to rely on consent for processing and when to look at alternatives. It also explains what counts as valid consent, and how to obtain and manage consent in a way that complies with the GDPR.

Documenting the legal basis for processing

The ICO has also recently issued guidance stating that data controllers must keep a record of the legal basis they are relying on for each element of processing, together with a justification as to why that basis applies. In addition, where data controllers are relying on legitimate interests, the ICO says that a "legitimate interests assessment" should be undertaken to help evidence compliance. The trustees' data audit / mapping exercise should help here.

The ICO has published templates to help data controllers and processors meet these record keeping requirements.

Data protection annual fee

All data controllers (unless exempt) must pay an annual fee to the ICO. This fee replaces the requirement for data controllers to "register" with the ICO, although they will still need to provide the ICO with certain information (either online or by phone on 0303 123 1113).

The new fee is arranged in three tiers, of £40, £60 or £2,900. Trustees will generally be required to pay a fee, with most expected to fall within the lowest band. The ICO has published a guide to help data controllers in working out what fee, if any, they are likely to pay. The guidance notes that payments by Direct Debit will attract a £5 discount.

A transitional period applies, so that data controllers with a current registration under the DPA will not have to pay the new fee until their existing registration expires. Trustees who are registered with the ICO can expect to receive correspondence confirming the new fee level.

Enforcement and sanctions

The ICO has a number of tools to help it, when necessary, "change the behaviour of organisations and individuals" that collect, use and keep personal data. These include powers to:

- issue warnings to a data controller or processor that their intended processing operations are likely to infringe the GDPR
- issue reprimands to a data controller or a processor where processing operations have infringed the GDPR
- order compliance with data subject requests to exercise their rights
- order communication of the breach with the data subject(s)
- impose administrative fines that are "effective, proportionate and dissuasive".

Fines of up to €20,000,000 (£17,000,000) or 4% of an organisation's global turnover may be imposed at the discretion of the ICO, in addition to or instead of other corrective measures, depending on the nature of the personal data breach and the circumstances of each case.

Whilst the ICO has not produced guidance with workplace pensions specifically in mind, its draft regulatory action policy notes that it will act proportionately when considering whether to take action, targeting its most significant powers at organisations and individuals "suspected of repeated or wilful misconduct or serious failures to take proper steps to protect personal data".

The new Data Protection Act

With the aim of ensuring the continued free flow of personal data around the EEA post-Brexit, the UK's new Data Protection Act 2018 received Royal Assent on 23 May 2018, and brings the GDPR into UK legislation (subject to certain amendments) from 25 May 2018.

The new Act brings with it some easements designed to allow the processing of sensitive personal data in certain circumstances.

One such circumstance is where the processing is “necessary for the purposes of performing or exercising obligations or rights” imposed by law “in connection with employment, social security or social protection”. Where this applies, the data controller will need to put certain safeguards in place, including an appropriate policy document and processing record. This easement should help employers when complying with their employment law obligations.

Whilst a further easement is stated to apply to the processing of sensitive personal data by occupational pension schemes, the provision is narrowly drafted and, despite its title, is only likely to be of use in very limited circumstances, such as where medical underwriting is being undertaken.

This is just the beginning…

As the ICO said recently, when it comes to compliance with the GDPR, “25 May is not the end. It is the beginning”.

Trustees have been working hard to update their systems, processes and contracts in line with the new legislation. But the obligations are ongoing, and the ICO will no doubt issue further guidance as thinking develops.

As the new requirements bed down, trustees should take stock over the next six to twelve months of how their revised processes are working and any new developments.

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