Sackers

Getting ready for the GDPR: countdown to 25 May 2018

Alert | 25 May 2017

Introduction

A major shake-up of European data privacy laws is on the horizon, with the General Data Protection Regulation (GDPR) coming into force on 25 May 2018. And with just 12 months to go, the clock is now ticking for trustees, employers and pension providers to get ready.

Key points

- Creation of a unified regulatory data protection regime, fit for the digital age, is the main aim of the GDPR.
- While many of the GDPR's provisions are familiar, there are new requirements, as well as tougher sanctions for non-compliance.
- The Government has confirmed that the UK's decision to leave the EU will not affect the UK's implementation of the GDPR in 2018.

What data does the GDPR apply to?

Information by which an individual can be identified

Under the GDPR, personal data is any information relating to a living individual which enables that individual to be identified, either directly or indirectly. In the pensions context, names, addresses and NI numbers, or any other information specific to their identity, as well as information relating to physical, social and cultural factors, all count as personal data.

Special categories of personal data

The concept of "sensitive personal data" in the DPA is rebranded under the GDPR as "special categories of personal data". This personal data attracts additional protection because it relates to information that is very personal, and/or because there may be greater risk to the individual if it is not processed as it should be or if data security is not maintained. Special categories of personal data include data relating to mental or physical health, racial origin, and sex life or sexual orientation.

For pension schemes, this type of personal data is most likely to be relevant when dealing with ill-health, divorce and death cases.

The data protection principles

The main principles to apply when processing personal data are:

Purpose

Personal data must be collected for specified, explicit and legitimate purposes.

Trustees need to consider the purpose for which personal data is collected, so this can be recorded and communicated to members. Identifying the purpose also enables schemes to check that personal data is being processed consistently with that purpose.

Data minimisation

Personal data must be adequate, relevant and limited to what is necessary for the purpose.

Personal data is needed in order to administer a scheme and to enable decisions to be made. The requirement to minimise data needs to be balanced with trustees' responsibilities, which include making decisions based on relevant and comprehensive information, and the need to ensure that legal and tax requirements are met.

Accuracy

Personal data should be accurate and up-to-date.

As good quality data is needed for pension schemes to function well, this is nothing new.

Storage (or security) limitation

Personal data should be kept for no longer than is necessary for the purposes for which it is held and processed.

Pension schemes are long-term arrangements and, as such, some personal data will need to be retained for many years so that benefits can be provided. It may also be necessary to retain personal data beyond certain events, such as a member transferring his/her benefits out of the scheme, to ensure that any questions or complaints arising in the future can be dealt with.

Trustees will need to explain their policy on data storage to members. In most instances, it will not be possible to identify a fixed time limit that will apply to storage of personal data by a scheme. Instead, trustees will need to explain the approach taken when determining how long to retain personal data for. Trustees will also need to record their policy on storage limitation.

Integrity and confidentiality

Personal data must be processed in a manner that ensures appropriate security of the data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Accountability

Under a new accountability principle, trustees (as data controllers) will be responsible for demonstrating compliance with the data protection principles.

The grounds for processing

Trustees need to determine the basis on which the personal data they hold is processed. For the processing of personal data to be lawful, it must meet at least one of six conditions (to which EU Member States can also add their own).

Conditions relevant to pension schemes include:

- the processing being necessary for the purpose of 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)
- complying with a legal obligation to which the trustees (as data controllers) are subject
- the processing being necessary for the performance of a contract, for example, paying benefits due under the scheme
- the member having given their consent to the processing of their data for one or more specific purposes.

Obtaining consent

The GDPR introduces more stringent requirements on how individuals should give their consent to data processing. Consent will have to be “freely given, specific [and] informed”. Essentially, it will not be possible to infer consent, for example, from pre-ticked boxes or a failure to provide a positive response. Once given, consent can be withdrawn at any time.

As noted above, consent is a basis that can be used for processing data. It is also required where special categories of personal data are being processed. However, additional requirements and individual rights apply where consent is used as the basis for processing.

Trustees should identify when they need to obtain consent. They should also review how they obtain consent and whether any changes to their procedures are required.

Communicating with members

The GDPR will introduce new information requirements which, among other things, will require trustees to issue information notices (also known as privacy statements). Information which will need to be given in the privacy statement includes:

- the identity of the data controller (generally, the trustees) and contact details
- the purpose of processing
- the legal basis for processing. If this is a “legitimate interest”, the legitimate interest should be stated
- who receives the data
- the period for which data is retained
- information about transfers of data outside of the EU / EEA

- relevant individuals' rights in respect of the data, and
- the right to complain to the ICO.

How we can help

We are producing a series of Alerts on the different elements of the GDPR in the countdown to May 2018 – you can read our general introduction to the new requirements here.

We can also help trustees get ready now for the GPDR in any number of ways, including:

- identifying the key questions to address so as to audit your current data
- reviewing existing or new contracts
- considering the policies and procedures you may need to put in place or update
- communicating with members.

For assistance with the above, or any other GDPR help you may need, 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