Sackers

Getting ready for the GDPR: the data protection principles

Alert | 19 September 2017

Introduction

The General Data Protection Regulation (GDPR) will introduce significant changes to data protection requirements from 25 May 2018. Whilst the data protection principles are broadly similar to those under the Data Protection Act 1998 (the DPA), there are some important revisions and additions being made by the GDPR.

Key points

- The GDPR revises the data protection principles which govern the processing of personal data.
- A new accountability principle requires trustees (as data controllers) to demonstrate compliance, and trustees should consider taking a number of practical steps now to help minimise the risk of breaches.
- A new Data Protection Bill was given a first reading in the House of Lords on 13 September 2017, with the aim of making "data protection laws fit for the digital age… and [empowering] people to take control of their data".
- Whilst the Bill will replicate much of the GDPR, it will also introduce a number of supplementary changes. We will be issuing a separate Alert on the Bill.

Lawfulness, fairness and transparency

Principle: personal data should be processed lawfully, fairly and in a transparent manner.

What does "lawfulness and fairness" mean in practice?

Data controllers need to have a lawful basis or ground for processing all personal data and they must keep records of what it is / they are (there may be more than one). Whilst "fairness" is not defined as such in the GDPR, the processing being carried out needs to be fair when balanced against the individuals' fundamental rights and freedoms.

Non-sensitive personal data

The grounds for processing (non-sensitive) personal data which are most likely to be relevant in a pensions context are:

- *Legitimate interests* – the processing is necessary for the purposes of the legitimate interests pursued by the data controller or a third party (such as the effective running of the pension scheme by the trustees and the scheme administrator). Members must be informed of the legitimate interests relied on and can object to processing on these grounds, although trustees can continue processing where there are compelling reasons.

- *Compliance with legal obligations* – to which the trustees (as data controllers) are subject. For example, trustees are required by law to keep certain information and records relating to scheme members and beneficiaries.

- *Contractual obligations* – personal data can also be processed where the processing is necessary for the performance of a contract to which an individual is a party or where steps are taken prior to entering into a contract at the individual's request. This is most likely to be relevant to employers (for example, in fulfilling their automatic enrolment obligations) and to contract based arrangements.

- *Consent* – personal data can also be processed if a member (or beneficiary) has given their explicit consent to the processing of their personal data for one or more specific purposes. The GDPR imposes stringent conditions for obtaining valid consent and, for this reason, the ICO suggests using consent as the ground for processing personal data only where necessary.

Sensitive personal data

Sensitive personal data (known as "special categories of personal data" under the GDPR) includes information relating to someone's health, racial origin, religious belief, politics, sex life or sexual orientation.

Obtaining consent is most likely to be relevant to trustees when they are processing sensitive personal data as part of dealing with an ill-health, death or divorce case. Other lawful grounds for processing sensitive personal data which may be relevant include where it is necessary to carry out certain employment obligations (this will be relevant to employers) or where the processing is necessary "for the establishment, exercise or defence of legal claims".

Transparency

The GDPR places a greater emphasis on communicating with individuals.

Trustees, as data controllers, will need to provide certain information to scheme members about the personal data they hold. This includes explaining why their personal data is needed, and how and by whom it will be processed. To satisfy the transparency requirement, member communications should use clear and plain language that is easily understood. Special care will also need to be taken where the recipient is a child.

Purpose limitation

Principle: personal data should be collected for "specified, explicit and legitimate purposes" and not further processed in a way that is incompatible with those purposes.

This means that trustees need to consider the purpose(s) for which they are collecting personal data, record this and let members know. Exact purposes for collecting and processing personal data may vary from member to member and change over time (eg as limits are imposed or flexibilities are introduced).

Recording the purpose(s) for processing will enable trustees to check that personal data continues to be processed in a way that is consistent with the original purpose(s).

Put simply, the main purposes for which personal data is likely to be collected by a pension scheme are to enable trustees to properly administer the scheme and to calculate and pay benefits.

Data minimisation

Principle: personal data should be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

Essentially, "data minimisation" means trustees collecting and using only the personal data they need for the purpose(s) they have identified. Inevitably, trustees need to collect and use certain personal data to administer the scheme properly. In practice, this will mean trustees:

- striking a balance between gathering information needed to make decisions, to pay benefits and to comply with their legal obligations generally, and not having more personal data than required
- avoiding the proliferation of copying where it is not strictly necessary and / or sharing personal data with others (such as advisers) where they do not need it to advise
- bearing in mind that information may be required to check that someone is not eligible for a particular benefit.

Accuracy

Principle: personal data should be accurate and, where necessary, kept up-to-date.

Good quality data is fundamental for pension schemes to function well, so the GDPR's requirement about accuracy should be nothing new.

In its record keeping guidance, TPR recommends that pension scheme data is checked annually to ensure that it is complete and accurate. In contrast, under the GDPR, every reasonable step must to be taken to ensure that inaccurate personal data is deleted or rectified without delay. Trustees should therefore have a plan in place to regularly review the personal data they hold.

Storage limitation

Principle: personal data should be kept in a form which permits an individual's identification for no longer than is necessary for the purposes for which the personal data is processed.

To meet the requirements of both UK tax and pensions law, trustees must keep certain information for a minimum of 6 years. But, given the long-term nature of pension schemes, the trustees may be required to keep personal data for at least the member's lifetime. Even after key events (such as a transfer out of someone's benefits or their death) questions, claims and challenges can often arise some years later.

The key is for trustees to have a policy in place under which personal data is regularly reviewed and, only if it is no longer needed, destroyed. Trustees will also need to explain their approach to members.

Integrity and confidentiality

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

As data controllers, trustees are responsible for keeping personal data safe. Suitable systems and processes should therefore be in place to ensure appropriate security. This is something for the trustees to raise with their scheme administrators, as well as other third parties with whom personal data is shared (eg actuaries and payroll providers).

Accountability

Principle: data controllers will be responsible for, and must be able to demonstrate compliance with, the data protection principles.

This is new and places a direct responsibility on the data controller for ensuring compliance with the data protection principles. Steps that trustees can take to fulfil their obligations here include:

- undertaking appropriate training and checking that their advisers have also done so
- carrying out audits to check what personal data they hold, who holds it, on what basis it is held, for how long and whether the trustees still need it
- 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.

How we can help

We are producing a series of Alerts on the different elements of the GDPR in the countdown to May 2018. In addition, we have produced a checklist on "Assessing pension scheme data – the questions trustees need to ask" which is available via our website.

We can also 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