Sackers

Getting ready for the GDPR

Individuals' rights

April 2018

Introduction

The General Data Protection Regulation ("GDPR") is set to come into force across the EU on 25 May 2018, and the Data Protection Bill which will implement it is nearing the end of its Parliamentary scrutiny.

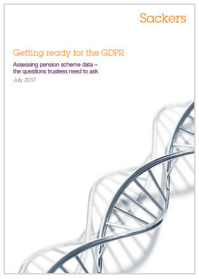
This checklist, the third in our series, sets out key questions and actions that trustees of occupational pension schemes should be addressing now to help protect and meet individuals' rights. It may also be of use to employers and in-house teams holding scheme membership data.

In this edition, we cover the following:

- general considerations when dealing with individuals' rights
- the new information requirements
- rights to access (and portability)
- the right to be forgotten and to withdraw consent
- a data subject's other rights
- summary
  - the new data protection principles
  - key terms.

Trustees can complete the information themselves or, for assistance, please get in touch with your usual Sackers contact or a member of our data protection team at: dataprotection@sackers.com.

Other checklists in this series



Checklist 1

Getting ready for the GDPR – assessing pension scheme data

Checklist 2

Getting ready for the GDPR – governance and contractual requirements

Notes

- References to "the GDPR" in this checklist will generally include the requirements of both the GDPR and the Bill (where applicable).
- References in this checklist to personal data and/or sensitive personal data held in respect of "members" of a pension scheme should be read as including any such personal data held in respect of dependants and beneficiaries (both actual and potential).
- Key questions and actions are denoted by "**Q**" and "**A**" respectively.

Part 1
General considerations when dealing with individuals' rights

Background

As data controllers of all scheme personal data, the trustees will be responsible for meeting individuals' rights under the GDPR. In reality, however, they will need assistance from others, chiefly the scheme administrators.

The general lawfulness, fairness and transparency principle (see Part 6) plays a key role when it comes to protecting individuals' rights under the GDPR. Put simply, all communications must be in a "concise, transparent, intelligible and easily accessible form, using clear and plain language" that is easily understood by the recipient. Unsurprisingly, extra care needs to be taken when communicating with children.

Costs

All information should generally be provided to data subjects free of charge, although the trustees (as data controllers) can charge a reasonable fee, or even refuse to act, where a request is "manifestly unfounded or excessive". However, the onus for demonstrating this will lie with the trustees.

Timescales

Trustees will generally need to respond to requests to exercise the individuals' rights outlined in Parts 3 to 5 of this checklist "without undue delay and in any event within one month of receipt of the request". However, this period can be extended by two further months where necessary, "taking into account the complexity and number of the requests". Trustees will need to inform the relevant individual of any such extension (within the initial one month timeframe), giving reasons for the delay.

Procedures and contracts

Given the costs potentially involved in meeting individuals' rights, and the tight timescales for complying, having a clear process in place will be essential.

The trustees' data protection policy will be the main document for recording how trustees look after personal data in relation to the scheme, reflecting key decisions taken and procedures put in place. Individuals' rights can either form part of this policy or trustees may prefer to have a standalone document.

In either case, trustees should aim to discuss their policy with their scheme administrators (as well as other key holders of personal data) and ensure that agreed contractual terms are compatible.

Joint controllers

Where trustees act as joint data controllers with another (such as the scheme actuary), they will need to consider how best to address individuals' rights. This is because, where there are joint controllers, a contract (or arrangement) must be in place setting out the parties' respective responsibilities for complying with the GDPR. A summary of this then needs to be provided to members.

Trustees in this position will therefore need to consider whether a joint privacy notice, and a single point of contact for dealing with individuals' rights, is warranted.

Part 2
The new information requirements

Summary

- Whilst there are similarities with current legislation, the GDPR will expand the range of information which must be given to data subjects. Trustees will need to review and update (as necessary) the scheme privacy notice to reflect these requirements.
- The information which will need to be covered includes:
  - the identity of the data controller and contact details
  - the purpose(s) of the processing
  - the legal basis relied on to justify processing (see Part 2 of Checklist 1)
  - if the legal basis includes "legitimate interests", details of them (members will have the right to object to processing on these grounds, see Part 5 below)
  - where information is not collected directly from the data subject, the categories of personal data involved and the source (including publicly accessible sources)
  - who personal data is shared with (specifying either the individual recipients or the categories of recipient)
  - information about transfers outside of the European Economic Area ("EEA"), including details about the safeguards put in place and where copies can be obtained
  - the period for which personal data will be stored or, if this is not possible, the criteria used for determining that period (known as "the retention period")
  - details about individuals' rights (see Parts 3 to 5 below)
  - the right to complain to the ICO
  - where applicable, details about any automated decision making (decisions made by computers rather than a human being) and any profiling of data subjects (both are more likely to be relevant to some providers than to trustees)
  - if relevant, contact details for the DPO (it is unlikely that trustees of occupational pension schemes will need to appoint a DPO, although providers and other advisers may need to do so – see Part 2 of Checklist 2).
- Trustees will need to decide how best to deliver the above information. Ideally, the same delivery method should be used across the communications piste so that there is consistency.
- The ICO's code of practice on privacy notices provides practical help here, recognising that information can be provided face-to-face, by post, or electronically (eg by email or by signposting to a website). A privacy notice need not be confined to a single document, as a layered approach can help to provide key information immediately with more detail available elsewhere.
- Whilst the timescales for providing a privacy notice vary depending upon whether the information is obtained directly from the data subject or indirectly from another source, the safest approach is to make it available at the time of collection (if not earlier). For new joiners, this will mean providing relevant information at the outset, as part of the joining process.

Key Questions & Actions		Date Completed
Q	Do existing communications with scheme members cover the privacy information required by the GDPR?	
Q	If not, is there a plan in place to review, update and distribute new privacy notices in line with the GDPR?	
Q	If relying on legitimate interests as the legal basis for processing personal data, are these explained in the privacy notice?	
Q	Do the trustees act as a joint data controller with any third party (such as the scheme actuary)?	
Q	If yes, will a joint privacy notice be issued or will members be signposted to a separate notice produced by the third party (see Part 1 above)?	
Q	As part of their data audit, have the trustees established whether any providers / advisers transfer scheme personal data outside of the EEA?	
Q	Have trustees sought legal advice on devising a suitable retention policy?	
A	Review existing communications and seek legal advice on updating the scheme privacy notice.	
A	Ensure that individuals are informed about the rights outlined in Parts 3 to 5 below.	

Part 3
Rights to access (and portability)

Summary

- As under current legislation, the right to access under the GDPR allows data subjects to ask a data controller whether their personal data is being processed. If so, except where it would adversely affect the rights and freedoms of others, the individual should be provided with a copy of that personal data accompanied by supporting information.
- In many ways, the supporting information mirrors the general information requirements (see Part 2 above). So, for example, individuals must be told the purposes of the processing, the categories of personal data involved, the parties to whom personal data has been (or will be) disclosed and, where personal data is not collected directly from the data subject, any available information as to its source. The rights to be forgotten, to rectification, and to restrict and/or object to processing outlined in Parts 4 and 5 below must also be covered.
- Whilst trustees can design a subject access form to be completed by members making such a request, ICO guidance makes clear that members must be free to choose their own means of communication, provided it is in writing.
- Where a subject access request is made electronically, unless requested otherwise, trustees should generally respond using the same medium. (In certain circumstances, an individual can require their personal data to be provided either directly to them or to a new data controller in a machine readable (ie portable) format.)
- When devising (or updating) their framework for dealing with subject access requests, some practical points for trustees to address include:
  - who is responsible for handling such requests – as data controllers, trustees are technically on the hook but, in reality, they will be heavily reliant on their scheme administrators and others
  - how to check that the person making the request is who they say they are – where trustees have reasonable doubts concerning an individual's identity, the GDPR makes clear that they can request additional information
  - having a process in place (eg by asking the individual concerned) for checking whether it is a formal subject access request or simply a general request for information, as dealing with the former will be more expensive and time consuming
  - how best to present the information requested.

Key Questions & Actions		Date Completed
Q	Do you have processes in place to deal with subject access requests (and, if applicable, portability) within the required timeframe (see Part 1 above)?	
Q	Are your scheme administrators equipped to help you deal with such requests?	
Q	If so, does your contract with the scheme administrators reflect that and the timescales for complying under the GDPR?	
Q	Are you / they able to provide copies of personal data in the formats required by the GDPR?	
A	Ensure that individuals are told about their rights to access and, if applicable, portability (see Part 1 above).	
A	Consider developing a standard process for dealing with subject access requests with your scheme administrators and legal advisers.	

Part 4
The right to be forgotten and to withdraw consent

Summary

Right to be forgotten

- An individual can request that a data controller erase personal data held in respect of him/her without undue delay where, for example:
  - the personal data is no longer needed for processing
  - he/she withdraws consent to processing (see below) and there are no other legal grounds for processing
  - he/she objects to processing (see Part 5 below) and there are no overriding legitimate grounds on which to continue
  - the personal data is being unlawfully processed.
- Where a data controller has shared personal data which it is obliged to delete with others, taking account of factors such as the cost of implementation, the data controller should take reasonable steps to inform the other parties.
- The right to be forgotten is subject to certain exceptions, such as processing being necessary to comply with a legal obligation. As trustees are required to pay benefits under the scheme, in the unlikely event a member (or a dependant or beneficiary) makes a request to be forgotten, trustees should generally be able to rely on this exception.

Right to withdraw consent

- The GDPR imposes new conditions for obtaining consent, including that it "should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of [his/her] personal data". The most likely circumstances in which consent will be required in a pensions context is where sensitive personal data is being processed in relation to ill-health, divorce or death cases (see Part 5 of Checklist 1).
- Members have the right to withdraw consent at any time. Withdrawing consent will not affect the lawfulness of any processing which took place beforehand and members will need to be informed of this before giving consent. It must be as easy to withdraw consent as it was to give it in the first place.

Key Questions & Actions		Date Completed
Q	Do you have a process in place to deal with any requests from members to be forgotten?	
Q	If relying on consent for processing any personal data, is there another legal ground you can use in the event a member withdraws that consent?	
Q	Are your scheme administrators equipped to help you deal with such requests?	
Q	If so, does your contract with the scheme administrators reflect that and the timescales for complying under the GDPR?	
A	Ensure that individuals are told about their rights to be forgotten and, if applicable, to withdraw consent (see Part 1 above).	
A	Consider developing a standard process for dealing with requests relating to individuals' rights with your scheme administrators and legal advisers.	

Part 5
A data subject's other rights

Summary

Right to rectification

- An individual has an unconditional right to have any inaccurate personal data held in respect of him/her rectified and, taking into account the purposes of the processing, to have any incomplete personal data updated. As good governance forms part of any well-run pension scheme, this requirement should come as no great surprise to trustees.

Right to object

- Where legitimate interests are relied on as the legal basis for processing personal data, members will have the right to object to such processing. An objection can be rejected by the trustees where there are "compelling" reasons which override the individuals' rights and freedoms.

Right to restrict processing

- A member can require the trustees to restrict the processing of his/her personal data, for example, whilst its accuracy is contested or where he/she has objected to processing based on legitimate interests (see above), pending checking whether there are compelling reasons to carry on.
- In these circumstances, personal data can be stored but not further processed without the individual's consent. Exceptions to this which are likely to be relevant to occupational pension schemes include where processing is necessary to protect someone else's rights (eg another beneficiary), or for establishing, exercising or defending a legal claim.

Right to be informed of a serious breach

- As well as being obliged to report personal data breaches to the ICO within 72 hours (where feasible), unless an exception applies, the data controller must also inform individuals "without undue delay" of any breach likely to result in a high risk to their rights and freedoms. A report must include details of the DPO or other contact point where further details can be obtained, and describe the likely consequences of the personal data breach, as well the measures taken or proposed to address it.
- Exceptions to the above requirement include where steps have been taken subsequent to the breach rendering it unlikely that a high risk will materialise.

Automated decision making

- Subject to limited exceptions (such as the decision being authorised by law), a member has a right not to be subjected to decisions based solely on an automated process, including profiling, which produce a legal or similarly significant effect. This is more likely to be relevant to providers than to trustees.

Key Questions & Actions		Date Completed
Q	Is scheme personal data regularly reviewed to ensure its accuracy?	
Q	Are your scheme administrators equipped to help you deal with any of the requests outlined above?	
Q	If so, does your contract with the scheme administrators reflect that and the timescales for complying under the GDPR?	
A	Tell individuals about the above rights (see Part 1 above).	
A	Consider developing a standard process for dealing with requests relating to individuals' rights with your scheme administrators and legal advisers.	

Part 6
Summary

The new data protection principles

Lawfulness, fairness and transparency – personal data should be processed lawfully, fairly and in a transparent manner

Data controllers need to have a lawful basis for processing all personal data and must keep records of what it is or 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. Trustees will need to provide increased information to scheme members about the personal data they hold. To satisfy the transparency requirement, member communications should use clear and plain language that is easily understood.

Purpose limitation – personal data should be collected for specified, explicit and legitimate purposes, and not further processed in a way that is incompatible with those purposes

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 – 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 involves trustees collecting and using only the personal data they need for the purpose(s) they have identified (ie running the scheme properly and paying benefits). Trustees should continue to collect the personal data they need but should keep data minimisation in mind when asking for information and sharing it, avoiding excess copying and/or sharing personal data with others (such as advisers) where it is not strictly necessary.

Accuracy – personal data should be accurate and, where necessary, kept up-to-date

Every reasonable step must be taken to ensure that inaccurate personal data is erased or rectified without delay. Trustees should therefore have a policy in place to regularly review the personal data they hold.

Storage limitation – personal data should be kept in a form which allows an individual's identification for no longer than is necessary for the purposes for which the personal data is processed

For both tax and pensions law purposes, trustees must keep certain information for a minimum of six years. But, given the long-term nature of pension schemes, trustees may find that it is necessary to keep much of the personal data for at least the member's lifetime. The key is for trustees to regularly review personal data and destroy anything which is no longer needed. Trustees will also need to explain their approach to members.

Integrity and confidentiality – 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. Trustees should therefore check that they and their scheme administrators, together with other relevant providers / advisers, have suitable systems in place to ensure appropriate security.

Accountability – data controllers will be responsible for, and must be able to demonstrate compliance with, the data protection principles

The main steps that trustees can take to fulfil their obligations here are set out in all three of our checklists.

Part 6
Summary cont.

Key Terms

Data controller – decides the purposes for and the means by which personal data is processed. They are responsible for ensuring that the processing of personal data complies with the relevant requirements of the GDPR and the law governing privacy in general. In the context of an occupational pension scheme, the trustees will be the data controller. However, certain providers / advisers and/or the scheme employer could be joint controllers alongside the trustees, or possibly even separate data controllers in their own right.

Data processor – is someone (other than an employee of the data controller) who processes personal data on behalf of the data controller. Scheme administrators and payroll providers will generally be data processors, as may advisers and other third party providers.

Data subjects – are individuals on whom personal data is held and, in the context of an occupational pension scheme, will include scheme members and, where relevant, their dependants and beneficiaries (both actual and potential).

DPIA – means a "data protection impact assessment" (see Part 2 of Checklist 2).

DPO – means a "data protection officer" (see Part 2 of Checklist 2).

ICO – means the Information Commissioner's Office, the UK regulatory body charged with ensuring compliance with data protection laws.

Personal data – is any information held in respect of an identified or identifiable living individual (or "data subject"). For this purpose, a person can be identified (directly or indirectly) in a number of ways including, in a nod to the 21st century, from an IP address. In a pensions context, personal data includes members' names, addresses, dates of birth, national insurance numbers, bank account and salary details etc.

Processing – is broadly defined and includes any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination (or otherwise making available), or destruction.

Pseudonymisation – means the processing of personal data in a way that the personal data can no longer be attributed to a specific individual without the use of additional information, provided that such additional information is kept separately and there are measures in place to ensure that the personal data is not attributed to an identified or identifiable individual.

Special categories of personal data (ie sensitive personal data) – includes personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, the processing of genetic and biometric data, as well as data concerning someone's health, sex life or sexual orientation.

Notes

Sackers

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