Sackers

Getting ready for the GDPR

Assessing pension scheme data – the questions trustees need to ask

July 2017

Introduction
Major shake-up of European data privacy laws on the horizon

With under 12 months to go until the General Data Protection Regulation ("GDPR") comes into force on 25 May 2018, the clock is ticking loudly for all organisations holding and processing personal data relating to individuals.

This checklist, the first in a series, sets out key questions and actions that trustees of occupational pension schemes should be addressing now to assess the personal data they hold. Whilst primarily aimed at trustees (and their administrators), this checklist may also be of use to employers and in-house teams holding scheme membership data.

The checklist covers the following areas:

- data protection principles
- lawful basis for processing
- new consent requirements
- children's personal data
- sensitive personal data
- key GDPR changes.

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.

Notes

- 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 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
Data protection principles

Summary

The GDPR revises the data protection principles, although they remain broadly similar to those set out in the Data Protection Act 1998 ("DPA").

- **Lawfulness, fairness and transparency** – personal data should be processed lawfully, fairly and in a transparent manner.
- **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.
- **Data minimisation** – personal data should be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.
- **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.
- **Storage limitation** – personal data should be kept in a form which allows an individual (ie a "data subject") to be identified for no longer than is necessary for the purposes for which the personal data is processed.
- **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.
- **Accountability** – data controllers will be responsible for, and must be able to demonstrate compliance with, the data protection principles.

Key Questions & Actions		Date Completed
Q	Have all trustees had appropriate training on the new requirements of the GDPR?	
Q	Have the trustees' in-house or external support teams (such as the pensions manager, the secretary to the trustees, the administrators etc) also had appropriate training?	
Q	Have you had confirmation from all service providers and advisers that their staff have received appropriate training on the new requirements?	
Q	Are all trustees familiar with the new data protection principles?	
Q	Whose personal data do you hold eg members, dependants and beneficiaries (both actual and potential)?	
Q	Is all personal data held in respect of the above processed in a way that is compatible with the specific purpose(s) (eg enabling benefits to be provided under the scheme) for which it was collected?	
Q	Is all personal data held by the trustees reviewed regularly to check that it remains relevant and limited to what is needed?	
Q	Is personal data accurate and up-to-date and only kept for as long as necessary?	
Q	Do you have a policy for reviewing personal data held and destroying what you no longer need?	
Q	Have all service providers and advisers confirmed that they have appropriate policies and procedures in place in light of the GDPR?	
A	Trustees should seek legal advice to review and update (as appropriate) all policies, procedures, and scheme documents which may have an impact on holding and processing personal data.	

Part 2
Lawful basis for processing

Summary

- The GDPR applies to the processing of personal data wholly or partly by automated means, as well as to the processing of personal data forming part of a filing system (or which is intended to form part of a filing system).
- Personal data is any information relating to a living individual (namely, the data subject) from which they can be identified, whether directly or indirectly. In a pensions context, personal data includes members' names, national insurance numbers, and other information that is specific to their identity. Information relating to physical, social and cultural factors is also personal data.
- Trustees must have a lawful basis for processing members' personal data. The legal bases which are most likely to be relevant to pension schemes 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 scheme administrator). Members must be informed of the legitimate interests on which processing is based (via the "information notice" or "privacy statement") and will have the right to object to such processing. An objection can be rejected by the trustees where there are "compelling" reasons
  - **compliance with legal obligations** – to which the trustees (as data controllers) are subject
  - **performance of a contract to which the individual is a party or steps taken (at their request) prior to entering one** – this will be more relevant to employers and also personal pensions
  - **consent** – 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 is being processed (see Part 5).
- As trustees must have a valid legal basis for processing personal data at all times, this may mean reassessing their reasons and whether they remain valid over time and/or where circumstances change.

Key Questions & Actions		Date Completed
Q	Are you clear about the legal basis (ie purpose) you rely on for processing all personal data?	
Q	Will these grounds still apply once the GDPR is in force?	
Q	Has the purpose for which you process any personal data changed over time?	
Q	If so, do you still have a legal basis for processing that personal data?	
Q	If relying on legitimate interests as the basis for processing any personal data, do you maintain records of your reasons for this so that, if a member objects to processing, you can demonstrate compelling reasons for continuing to process?	
Q	Would scheme members reasonably expect the trustees (or a relevant third party, such as the scheme administrator) to process their personal data on the basis of a legitimate interest?	
A	Audit your personal data (and request that your scheme administrators as data processors and any other relevant service providers and/or advisers do likewise) so as to check what you hold, who holds it, on what basis you hold it, how long you have held it and whether you still need it.	
A	Review (and update as necessary) your governance processes to ensure that you can demonstrate how decisions to use personal data for processing and further processing purposes have been reached.	
A	Where relying on legitimate interests, document any decisions made regarding the balance between the trustees' interests as the data controller and the members' fundamental rights and freedoms, particularly where this affects children (see Part 4).	

Part 3
New consent requirements

Summary

- The GDPR imposes new conditions for obtaining consent. Consent "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".
- When requesting consent, trustees must therefore use clear and plain language that is easy to understand. The request must also specify why the trustees need the personal data and explain all of the ways in which it might be used. The member should be able to indicate consent to all or any of the purposes for which his/her personal data might be used in a clear and simple way. A member should be able to refuse to consent without suffering any detriment.
- Consent can be given both orally and in writing (including via electronic means). This could include ticking a box when visiting a website or conduct which clearly indicates the member's acceptance of the proposed processing of his/her personal data. If a member's consent is given as part of a document dealing with other issues, the request for consent must be prominent and clearly distinguishable. Silence, pre-ticked boxes or inactivity will not constitute consent.
- 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.
- The most likely circumstance in which consent will be required is where sensitive personal data is being processed (see Part 5). Specific rules will also apply to children (see Part 4).
- As the Information Commissioner's Office ("ICO") notes in its draft "GDPR consent guidance", if obtaining consent is too difficult, trustees should consider whether another lawful basis for processing personal data is more appropriate.

Key Questions & Actions		Date Completed
Q	Do you need to rely on consent for processing personal data or can you rely on another legal basis for processing?	
Q	If you need to rely on consent, have you sought the specific consent of relevant members to holding and processing their personal data?	
Q	Does your procedure for obtaining consent (both past and present) meet the new requirements of the GDPR? Do you have any evidence of this?	
Q	If not: • is there a plan in place to refresh consents that do not meet the GDPR standard? • do you have an alternative lawful basis for holding and processing all relevant personal data? • is this personal data that needs to continue to be held?	
Q	Is there a clear and straightforward process in place allowing a member to withdraw his/her consent to processing their personal data?	
Q	Are there adequate procedures in place to ensure that, as soon as a member withdraws his/her consent to processing: • all affected parties (ie trustees and administrators as data controller and data processor respectively) are notified with immediate effect? • no further processing which relies on that consent takes place?	

Q Do you have a process in place for regularly reviewing consents and refreshing them to reflect any changes in circumstances?

A When updating data protection policies, consider setting out steps to help manage the practical implications of obtaining consent and the possibility of a member withdrawing their consent, including how this might impact the trustees' ability to make decisions about benefits.

A If you need to rely on consent for processing certain personal data, speak to your legal advisers about updating communications to ensure that:

- specific, informed and unambiguous consent has been/is given freely
- the language used when obtaining consent is clear, plain and easy to understand
- consent has not been/is not inferred, for example, by using pre-ticked boxes or by a member failing to provide a positive response
- where consent to processing personal data is sought as part of a larger communication, the request for consent is sufficiently prominent
- when seeking consent, members are made aware of all parties to whom that personal data (including any sensitive personal data) is likely to be disclosed
- members are informed that they have the right to withdraw consent to future processing at any time, although perhaps noting that this may affect the trustees' ability to distribute/make decisions about benefits.

A Put in place a standard process and form for obtaining consent, as well as a simple method for withdrawing consent.

A Keep records of all consents and the dates on which they were obtained, including copies of all communications leading up to consent being given.

Part 4
Children's personal data

Summary

- Unsurprisingly, children are regarded as being particularly vulnerable, therefore warranting "specific protection" under the GDPR. As processing personal data in relation to children is regarded as carrying extra risk, further restrictions may be imposed by codes of practice.
- When providing online services directly to a child and relying on consent as the lawful basis for processing personal data, the parent's or guardian's consent will need to be obtained for children below age 16. However, the UK could specify a lower age limit for this purpose, as long as it is not below age 13.
- Processing data relating to children offline will continue to be subject to the UK's rules governing the capacity of children to give consent.
- Consent of the parent or guardian is not required in the context of preventative or counselling services offered directly to a child.

Key Questions & Actions		Date Completed
Q	Do child dependants have access to online services offered by the trustees?	
Q	If so, do minimum age requirements apply?	
Q	Is the consent of the parent or guardian always sought where a child is under age 16?	
Q	Do trustees rely on "legitimate interests" as the legal basis for processing children's personal data (other than sensitive personal data)?	
Q	If so, are the reasons why there is a legitimate interest carefully thought out and documented, including consideration as to whether the child's interests might override those of the trustees?	
A	Trustees should check what, if any, personal data they hold in relation to children, what legal basis they have for processing it and that this is properly documented.	
A	If relying on legitimate interests, trustees should also consider with their legal advisers (and document this) whether the child's fundamental rights and freedoms might override those legitimate interests.	

Part 5
Sensitive personal data

Summary

- The grounds for processing sensitive personal data (referred to in the GDPR as "special categories of personal data") are broadly the same as those used in the DPA, but there are some changes. For example, special categories of personal data specifically include the processing of genetic and biometric data, such as finger prints and facial imaging, for the purpose of uniquely identifying an individual.
- Special categories of personal data also include data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, as well as data concerning someone's health, sex life or sexual orientation.
- For pension schemes, sensitive personal data is most likely to be relevant when dealing with ill-health, divorce and death cases.
- The GDPR generally prohibits the processing of sensitive personal data unless certain conditions are met, one of which is obtaining the individual's explicit consent. Others that may be relevant in the pensions context include where processing is necessary for:
  - carrying out employment law obligations and/or exercising specific rights
  - establishing, exercising or defending legal claims
  - assessing the working capacity of an employee.
- Processing is also possible where the personal data has been "manifestly made public" by the member.

Key Questions & Actions		Date Completed
Q	Do you hold information, such as on a nomination form or in relation to a particular scheme exercise, which might amount to sensitive personal data?	
Q	Do you hold any information in relation to members in general which reveals their racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, or data which could reveal details about their health, sex life or sexual orientation?	
Q	If so, do you have the member's explicit consent to holding that sensitive personal data?	
Q	If not, what legal basis do you have for processing that sensitive personal data?	
Q	Will it be possible to continue to process that sensitive personal data once the GDPR is in force?	
Q	Do you need to continue to hold existing sensitive personal data or can it be destroyed?	
Q	If you are relying on consent for processing sensitive personal data, does your procedure for obtaining consent (both past and present) meet the new requirements of the GDPR? (See Part 3)	
A	Audit your sensitive personal data (and request that your scheme administrators as data processors and any other relevant service providers and/or advisers do likewise) so as to check what you hold, who holds it, on what basis you hold it, how long you have held it and whether you still need it.	

Summary
Key GDPR changes

Background

The GDPR is designed to harmonise data protection law across the EU and to update the legislation to reflect advances in technology so as to make it fit for the digital age. While many of the GDPR's requirements are similar to those under the DPA, the new legislation will introduce a number of changes that will be relevant to pension schemes.

Despite Brexit, the Government has confirmed that the GDPR will apply in the UK from 25 May 2018 and so trustees, employers and pension providers should start preparing.

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 national insurance 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 role of data controllers and data processors

Data controllers

Data controllers decide the purposes for and the means by which personal data is processed. In the context of an occupational pension scheme, trustees are data controllers but it is possible for there to be joint data controllers in respect of the same data.

Under the GDPR, data controllers will need to be able to demonstrate that they comply with the legal requirements that are relevant to the personal data they control. It will no longer be necessary to register as a data controller with the ICO.

Where there are joint controllers, the GDPR sets out a stronger joint liability framework, with the new requirements including:

- the need to set out joint controllers' responsibilities in a transparent manner and to make a summary of this available to individuals whose personal data is held
- full liability resulting from a breach of the GDPR, unless one of the data controllers can show that it is not in any way responsible.

Data processors

A 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 pension payroll providers will process personal data on behalf of trustees, and advisers and other third party providers may also be data processors.

The GDPR will introduce requirements that will apply directly to data processors and it will be possible for data processors to be fined for breaches and be liable for compensation to individuals.

Communicating with members

The GDPR will introduce additional requirements relating to providing members with information. Schemes will need to issue information notices (also known as privacy statements), and it is likely that existing information will need to be updated. Points that will need to be covered in privacy statements include:

- the identity of the data controller and contact details
- the purpose of and legal basis for processing. If this is legitimate interests, the legitimate interest should be stated
- who receives the personal data
- the retention period for personal data
- information about transfers outside the European Union/European Economic Area
- relevant individuals' rights in respect of their personal data
- the right to complain to the ICO.

At a glance

Key changes to data protection law being made by the GDPR include:

- **right to be forgotten** – the GDPR gives individuals stronger rights to require that personal data held about them is removed
- **contract terms** – contracts will need to include specific terms relating to the storage and protection of data. This includes contracts between data controllers and data processors
- **reporting breaches** – serious breaches will need to be reported to the ICO within 72 hours where feasible and to individuals if the breach is likely to result in a high risk to their rights and interests
- **sanctions** – depending on the nature of the breach, the maximum penalty for non-compliance with the GDPR will increase significantly from the current maximum of £500,000 to the greater of €20,000,000 or 4% of the organisation's turnover
- **data protection officer** – organisations will be required to appoint a data protection officer if their core activities require "regular and systematic monitoring of data subjects on a large scale". This is unlikely to affect most occupational pension schemes but could potentially affect providers
- **consent** – the GDPR introduces more stringent requirements on how individuals should give their consent to data processing (see Part 3).

Notes

Sackers

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