Sackers

Getting ready for the GDPR

Governance and contractual requirements

December 2017

Introduction
Data privacy laws shake-up

The General Data Protection Regulation ("GDPR") is scheduled to come into force across the EU on 25 May 2018. In anticipation, the Government has now published a Data Protection Bill ("the Bill"), with the aim of incorporating the GDPR into UK legislation and ensuring the continued free flow of personal data in the post-Brexit world.

This checklist, the second in our series, sets out key questions and actions that trustees of occupational pension schemes should be addressing now in order to help ensure that their governance and contractual requirements (and those of their providers and advisers) are up to GDPR scratch. It may also be of use to employers and in-house teams holding scheme membership data.

In this edition, we cover the following:

- key governance obligations
- DPOs and DPIAs
- trustees' policies and procedures
- contractual requirements between data controllers
- contractual requirements between data controllers and processors
- 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. For the first checklist in the series, see Getting ready for the GDPR – assessing pension scheme data.

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
Key governance obligations

Summary

- Good governance plays a vital role under the GDPR. Whilst the main obligations fall squarely on a data controller's shoulders, data processors are also on the hook in some respects.
- Often overlapping, the governance measures under the GDPR are generally underpinned by a "proportionality" threshold, allowing a data controller / processor to take account of certain factors so as to focus on the areas where the risks are greatest and where action and effort will be most beneficial. Depending on the circumstances, the factors which may be taken into account include the scope and context of the processing, the cost of implementation, and the risks posed (both in terms of likelihood and severity) to an individual's rights and freedoms.

Data controllers

- As data controllers, trustees:
  - will be responsible for, and must be able to demonstrate compliance with, the data protection principles (see Part 6)
  - will need to determine the legal basis (ie the grounds) on which all personal data is processed, bearing in mind there may be more than one (see our first checklist)
  - must implement "appropriate technical and organisational measures" to ensure that all processing of personal data is performed in accordance with the GDPR, and that such measures are reviewed and updated where necessary
  - must implement "appropriate technical and organisational measures" to put in place an appropriate level of security (ie relative to the risk) when processing personal data. At the heart of this obligation is the need to protect the ongoing confidentiality, integrity and availability of personal data, having the ability to restore access to it in a timely manner in the event of a problem, and a process for regularly testing, assessing and evaluating the effectiveness of procedures
  - will need to provide individuals with certain information (in the privacy notice) and generally safeguard individuals' rights, such as the right to access information and the right to be forgotten.
- Appropriate "technical and organisational measures" could include the use of encryption and "pseudonymisation" (see Part 6) so that the individual cannot be identified.
- The GDPR also introduces the concepts of data protection "by design" and "by default". The former requires systems to be designed and deployed on a proactive (as opposed to a reactive) basis at the outset, so as to implement the data protection principles in an effective manner and to incorporate necessary safeguards to meet the requirements of the GDPR in general. Reinforcing the data minimisation principle (see Part 6), data protection "by default" requires that only personal data which needs to be processed is, in fact, processed, and that individual's personal data is not given to an indefinite number of people without the individual concerned being able to intervene.

Data processors

- The GDPR also places specific obligations directly on data processors, who play a key role in helping data controllers fulfil their governance obligations. As a consequence, under the GDPR, a binding contract must be put in place between a data controller and a data processor which satisfies certain minimum requirements (see Part 5).
- In common with data controllers, it will be possible for data processors to be fined for breaches and to be liable for compensation to individuals. A processor will also need to employ appropriate security measures to protect personal data.

Key Questions & Actions		Date Completed
Q	Have all trustees had training on the requirements of the new GDPR and on data privacy laws generally?	
Q	Have the trustees had confirmation from all in-house and external support teams (such as the pensions manager, the secretary to the trustees, the administrators etc), as well as relevant service providers / advisers, that their staff have received appropriate training on the new requirements?	
Q	Have trustees checked with their in-house and external support teams, as well as relevant service providers / advisers, what processes and procedures they have in place in order to support the trustees in meeting their governance obligations under the GDPR?	
Q	Does each trustee have appropriate security measures in place to protect personal data (including information held on computers and manual filing systems, on laptops, memory sticks and/or in paper form)? Are any changes needed (eg might a secure website be useful)?	
Q	Have you checked that your in-house and/or external support teams, as well as relevant providers / advisers, have appropriate security measures in place?	
Q	Before personal data is shared, do you consider whether all elements of it need to be shared?	
Q	When sharing personal data with others, do the trustees anonymise or encrypt this information (where possible) and ensure that others acting on their behalf do likewise?	
A	Audit your personal data (and ask that your scheme administrators and any other relevant service providers / 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	Trustees should consider the processes that they and others acting on their behalf have in place for ensuring the security and confidentiality of personal data.	

Part 2
DPOs and DPIAs

Summary

- Both a data controller and a data processor will be required to appoint a data protection officer ("DPO") in the following circumstances:
  - the processing is carried out by a public authority or body (subject to certain exceptions)
  - the data controller's / processor's core activities involve regular and systematic monitoring of data subjects on a large scale, or
  - the data controller's / processor's core activities consist of large scale processing of sensitive personal data and personal data relating to criminal convictions and offences.
- A data controller's (or processor's) "core activities" are its primary activities as an organisation. In an occupational pension scheme context, the trustees' core activities will be the processing of scheme membership data for the purposes of calculating and paying benefits.
- Given the above, 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. Nonetheless, trustees should consider whether a DPO is needed with their legal advisers and document their conclusions. Some trustees may even consider appointing a DPO on a voluntary basis. But trustees should beware appointing a DPO under the GDPR inadvertently, either by assigning all of the tasks which would be performed by a DPO to a single person, or by labelling a given individual as their DPO.
- Where a DPO is required, the role must be carried out by someone with expert knowledge of data protection law and practices, and he/she must report directly to the highest level of management. A DPO's responsibilities include monitoring compliance with the GDPR and relevant policies, as well as being the point of contact for the Information Commissioner's Office ("ICO").
- Whilst not a new concept (there is already an ICO code of practice), the GDPR formalises the requirement to carry out a data protection impact assessment ("DPIA") in specific circumstances. A DPIA is used to help identify and minimise privacy risks, and can also help to protect against reputational damage. It is more likely to be relevant to certain providers than to the trustees themselves.
- A DPIA must be carried out by a data controller prior to any processing which is likely to result in a high risk to individuals' rights and freedoms (eg when using new technologies and/or new types of processing operation), or where there is large scale processing of sensitive personal data. If a DPIA reveals that processing personal data will result in a high risk to individuals unless steps are taken to mitigate that risk, the ICO must be consulted before any personal data is processed.

Key Questions & Actions		Date Completed
Q	Have you considered whether you need to appoint a DPO and recorded your conclusions?	
Q	Do your scheme administrators and other advisers / providers need to appoint a DPO?	
Q	Do the scheme administrators and/or other providers / advisers have a process in place for identifying whether a DPIA is needed and for carrying one out if required?	
Q	Are the scheme administrators and/or other providers / advisers under an obligation to notify the trustees if they become aware of circumstances in which a DPIA is required?	
A	Trustees should ensure that relevant providers / advisers have a process in place for identifying whether a DPIA is needed and for carrying one out on the trustees' behalf.	

Part 3
Trustees' policies and procedures

Summary

- As data controllers, trustees will need to implement appropriate measures to comply with the GDPR, protect individuals' rights, reduce the risk of data breaches occurring, manage breaches that do occur, and to demonstrate that they are taking GDPR compliance seriously.
- With fines of up to €20 million (£17 million) or 4% of worldwide turnover a possibility, and with the data controller required to report a serious breach to the ICO within 72 hours (where feasible) and to individuals if it is likely to result in a high risk to their rights and interests, having effective policies and procedures in place will be essential for trustees.
- The 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 to meet GDPR requirements. A data protection policy's contents and structure will vary from scheme to scheme (eg there may be several policies dealing with discrete areas), but it should aim to cover certain points as a minimum. These include:
  - identifying the categories of individuals in respect of whom personal data is collected, the types of personal data, the purposes for which it is processed, the legal grounds relied on for processing, the parties with whom personal data is shared (and why), and the process for keeping all of these components under review
  - outlining how the trustees will meet the data protection principles
  - describing the procedures in place to safeguard the security of personal data, including cyber security, and the requirements placed on data processors acting on the trustees' behalf
  - explaining how access to and use of personal data is limited
  - addressing individuals' rights, including handling data subject access requests
  - dealing with transfers of personal data
  - setting out how trustees will manage breaches
  - documenting key decisions (eg regarding the appointment of a DPO) and the trustees' approach to record keeping generally
  - recording a clear process for monitoring and regularly reviewing all aspects of compliance with the GDPR, and for regularly training trustees.

Key Questions & Actions		Date Completed
Q	Have the trustees got an appropriate data protection policy and relevant procedures in place to ensure compliance with the GDPR and data privacy laws generally?	
Q	Have your scheme administrators' policies and procedures been updated in the 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.	
A	Trustees should keep appropriate records of the scheme's processing activities and ensure that the scheme administrator does likewise.	
A	Trustees should seek confirmation from all service providers and advisers that their policies and procedures are GDPR compliant.	

Part 4
Contractual requirements between data controllers

Summary

- The GDPR sets out specific requirements on how relationships should be documented where personal data is being shared between certain parties. The purposes for which personal data will be collected and used, and who is in the driving seat when it comes to deciding that, will be essential in determining the type of data sharing arrangement required.
- Parties may share personal data in one of three ways (which will, in turn, dictate the nature of the agreement which will need to be entered into between them):
  - **data controller to data controller** – this type of data sharing is commonly seen when trustees share information about scheme members and beneficiaries with the scheme employer
  - **joint controllers** – where two or more parties jointly determine the purposes and means of processing personal data, they will be "joint controllers". For example, owing to the nature of their role, the scheme actuary may be a joint controller alongside the trustees
  - **data controller to data processor** – for example, trustees to scheme administrators (see Part 5).
- There are no specific requirements in the current legislation, or in the GDPR, regarding documenting data sharing between separate data controllers, as each data controller is independently responsible for complying with the GDPR. That said, 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.
- Where there are joint controllers, the GDPR sets out a stronger joint liability framework, with the new requirements including:
  - putting a contract (or arrangement) in place to determine the joint controller's respective responsibilities for complying with their obligations under the GDPR, including meeting the information requirements to individuals (eg by a joint privacy notice) and dealing with individuals' rights
  - making a summary of the contract (or arrangement) available to members
  - full liability resulting from a breach of the GDPR, unless one of the joint controllers can show that it is not in any way responsible.
- Regardless of what any contract or arrangement says, members will be able to exercise their rights under the GDPR (eg to access information, to be forgotten, or to have inaccurate personal data corrected) against either joint controller.

Key Questions & Actions		Date Completed
Q	Do the trustees alone determine all of the purposes for and means by which personal data is processed in relation to the scheme?	
Q	If not, do they have a contract or arrangement in place with any joint controller setting out their respective obligations and liabilities which meets the requirements of the GDPR?	
Q	Do the trustees and the joint controller(s) have a clear process in place for communicating with members, dealing with members' rights and handling breaches under the GDPR?	
Q	Have the trustees and any joint controller nominated a single point of contact for dealing with queries from scheme members?	
A	Consider the services that your providers, advisers and the employer (including the pensions manager) provide involving the scheme's personal data, and discuss with them their understanding of their role so that their status as a data controller, joint controller or data processor can be confirmed and appropriately documented.	
A	Trustees who are joint controllers with another party should seek legal advice about documenting and managing that relationship.	

Part 5
Contractual requirements between data controllers and processors

Summary

- Under the GDPR, the contract governing the relationship between a data controller and a data processor is subject to more stringent requirements than under current legislation. Whilst some features of the data controller and data processor requirements will be familiar, others will require significant changes to existing contracts. The ICO's draft guidance, Contracts and liabilities between controllers and processors, provides useful analysis and a helpful checklist.
- There will need to be a binding contract in place between the trustees (as the data controller) and any data processor (eg the scheme administrator) whose services they engage, setting out the subject matter and duration of the processing, the nature and purpose of the processing, the types of personal data involved, and the categories of individuals on whom it is held.
- Using the example of a scheme administration agreement, some other essential elements of the new contractual requirements include the need for the scheme administrator to:
  - as per current legislation, act only on the trustees' written instructions, unless otherwise required by law
  - ensure that persons authorised to process personal data are obliged to keep it confidential
  - implement appropriate measures to ensure the security of processing
  - assist the trustees in meeting their security obligations under the GDPR, as well as in notifying breaches and carrying out a DPIA (if required)
  - assist the trustees in dealing with members' rights, for example, a data subject access request
  - delete or return all personal data to the trustees at the end of the contract
  - engage a sub-processor only with the trustees' prior written agreement and having imposed similar contractual requirements on the sub-processor (the administrator will remain fully liable to the trustees for any breach by the sub-processor)
  - make all information needed to demonstrate compliance with relevant obligations of the GDPR available to the trustees
  - allow for, and contribute to, audits carried out by the trustees or someone else on your behalf.
- Trustees should only use scheme administrators and other providers / advisers who provide sufficient guarantees that they have implemented appropriate technical and organisational measures so as to ensure that their processing of personal data meets GDPR requirements and the protection of individuals' rights.
- In addition to ensuring that contract terms meet GDPR compliance requirements, trustees should also consider whether terms relating to liability (including any limits on liability) and allocation of risk are appropriate.

Key Questions & Actions		Date Completed
Q	Have the scheme administrators and other providers / advisers who are data processors provided the trustees with sufficient guarantees that they will / have implemented appropriate technical and organisational measures so as to meet GDPR requirements?	
Q	Has the trustees' contract with the scheme administrators and other providers / advisers who are data processors been updated in light of the GDPR?	
Q	Do the scheme administrators regularly update the trustees on their performance under the contract, including steps taken to comply with the GDPR?	
Q	Do the scheme administrators (or any other providers / advisers) delegate any aspects of the processing of personal data in relation to the scheme to a sub-processor? If so, have the trustees agreed to this?	
Q	Do the scheme administrators have appropriate record keeping procedures in place to help the trustees meet their GDPR obligations, including dealing with members' rights (eg data subject access requests) and notifying breaches to the ICO and/or members if required?	
Q	Have the trustees considered whether there are any other parties (including individuals assigned by the employer to help the trustees) who may be processing personal data on their behalf?	
A	Consider the services that your providers, advisers and the employer (including the pensions manager) provide involving the scheme's personal data, and discuss with them their understanding of their role so that their status as a data controller, joint controller or data processor can be confirmed and appropriately documented.	
A	Trustees should seek legal advice to review and update (as appropriate) the contract with their scheme administrator and other providers / advisers who process personal data on their behalf.	

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 Parts 1 and 3 of this checklist.

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).

DPO – means a "data protection officer" (see Part 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 different 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.

Sackers

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