STEPHENSON HARWOOD

GDPR and pension schemes

What trustees need to do

The European General Data Protection Regulation ("GDPR") comes in to force on 25 May 2018 and heralds a step change in data protection ("DP") law throughout the European Union. The GDPR is due to be implemented in to national law through a new DP act (which is yet to be published) so the UK can meet its DP obligations both before and after Brexit.

To ensure compliance with the new DP law by 25 May 2018, it is vital that trustees:

- take stock of their current DP practices now
- understand the impact of the changes to DP law for them and on their scheme
- take any necessary action.

Where do trustees start?

Here. This document sets out our 8 point DP check for trustees. The starting point for trustees should be a data audit, as this will go some way towards satisfying the new requirements and help identify what other steps they need to take. This should be undertaken as soon as possible and no later than the end of October 2017 to ensure full compliance by May 2018.

Key points for trustees to address as part of this process are:

- scheme privacy notices (to ensure they meet the new requirements)
- a review of trustee liability protection in light of the harsher penalties that may apply for non-compliance with DP legal requirements
- a review of the legal basis adopted for processing personal and sensitive data
- shorter timeframes for complying with subject access requests and reporting any data breaches to the Information Commissioner's Office ("**ICO**")
- new rights for members to request deletion of personal data
- reviewing third party service provider agreements to ensure compliance with the new DP requirements.

Stephenson Harwood has a DP Toolkit to help trustees navigate their initial data audit and address the above points. Full contact details of our team members are on the last page should you wish to find out more about our DP Toolkit or if you have any general DP queries arising from this document.

1. Information held by trustees

Under the existing DP law, there is an is implicit requirement that trustees know what data they hold and how that data is held. The GDPR makes this an *explicit* requirement, requiring trustees to document the data they hold, the source of that data and who it is shared with.

By doing this, trustees may discover certain DP issues that need to be addressed. For example, trustees may identify certain data that is not necessary and make arrangements for its deletion.

To comply with this new requirement properly, trustees should consider carrying out a data audit covering:

- **The personal data held**
- **The source of that data**
- **How the data is stored, where it is stored and how long for**
- **The reason(s) it is necessary to process that data**
- **Whether it is legitimate to process that data**
- **Who else has access to the data**

2. Communicating privacy information

Trustees should already use privacy notices which provide fair processing information to members and which might also seek express consent to the processing of personal and sensitive personal data.

The GDPR enhances the existing requirements so that it will be necessary for trustees to communicate:

- The reason(s) and the legal basis which they are relying on to process personal data.
- How long the data will be held for.
- Information about the right to complain to the ICO where individuals think there is a problem with the way their data is being handled.

All notices must be concise, transparent, intelligible and easily accessible.

Trustees will need to review their existing privacy notices and update them in line with the new requirements.

3. Data rights (including subject access requests)

The current DP law already provides certain rights to pension scheme members and beneficiaries over the personal data trustees may hold about them. This includes a right to access their personal data and rights to stop certain data processing.

The GDPR makes significant enhancements and additions to these data rights, including a new right to delete personal data where continued processing is unnecessary (not just where damage or distress is caused). In addition, the subject access request ("**SAR**") requirements are being made more onerous so that:

- The time for compliance with any SAR is reduced from 40 days to one month.
- The ability to charge a £10 fee for any SAR is now much more limited.
- It is possible to refuse, or ask for a reasonable fee for, unfounded or excessive SARs but prescribed information must be provided to the data subject in such circumstances.

Trustees should consider how their procedures should change to comply with these enhanced requirements.

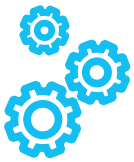
4. Member consent

Consent to the processing of personal data will generally become more difficult to obtain. For example, it must be freely given, specific, informed and unambiguous. There must also be a positive opt-in and so it will not be possible to infer consent from silence, pre-ticked boxes or inactivity. Requests for consent that are bundled in with other terms, rather than clearly separated out, will probably not be sufficient.

Trustees who rely on consent to process data will need to review existing consents to determine whether they would be adequate under GDPR. Privacy notices in existing application forms and member booklets may not be adequate and so a new GDPR-compliant consent mechanism may be required.

Members will have the right to withdraw consent at any time and this could potentially create significant operational issues for schemes. In addition, GDPR-compliant consent may be difficult to obtain for schemes which are used to satisfy employers' auto-enrolment obligations. As such, trustees may need to look for a different legal basis for processing personal data.

5. Legal basis for processing personal data



The legal basis (or bases) adopted for processing personal data will be more of an issue under the GDPR, as some individuals' rights will be modified depending on the legal basis adopted. For example, if trustees rely on member consent, the members will generally have stronger rights, including a right to have their data deleted.

Alternatives to member consent for non-sensitive personal data include where processing is necessary for the performance of a contract with the member or for the purposes of legitimate interests pursued by the trustees (except where those interests are overridden by the interests, rights or freedoms of the member).

Trustees need to determine the legal basis on which personal data is processed, document this and update the relevant privacy notices to explain it.

6. Accountability – demonstrating compliance

The GDPR includes an accountability principle which effectively means trustees must not only comply with the data protection principles but also demonstrate how they comply.

Trustees can take a number of steps to help ensure and demonstrate compliance:

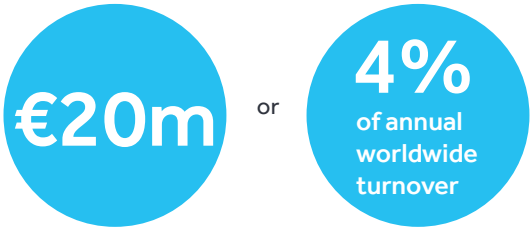
- Keep records of all data processing activities carried out.
- Implement (or review existing) technical and organisational measures for achieving compliance, e.g. data protection policies in relation to trustee training and internal audits of processing activities.
- Undertake a data protection impact assessment **("DPIA")** where data processing is likely to result in high risk to individuals, e.g. where new technology is being deployed. Trustees could prepare a DPIA policy/template document.
- Implement measures that meet the principles of data protection by design and by default, including data minimisation, pseudonymisation, transparency, and improving security features on an ongoing basis.

7. Data breaches and fines for breaches

A personal data breach is a breach of security leading to the destruction, loss, alteration or unauthorised disclosure of, or access to, personal data.

There will be a new mandatory requirement for trustees to notify data breaches to the ICO where it is likely to result in a risk to the rights and freedoms of individuals (e.g. where a breach could result in discrimination, damage to reputation or financial loss). Notifications must be made without undue delay and, where possible, within 72 hours of becoming aware of the breach. If the breach is likely to result in a high risk to the rights and freedoms of individuals, the trustees must also notify the individuals concerned directly without undue delay.

Failure to notify can result in a fine of up to the higher of €10 million or 2% of annual worldwide turnover. This would be in addition to the fine for the breach itself, which could be up to the higher of €20 million and 4% of annual worldwide turnover (a significant increase to the current maximum fine of £500,000).



While there is uncertainty about how "turnover" will be applied in relation to a pension scheme, and it is perhaps unlikely that the ICO would impose a heavy fine where doing so would ultimately penalise members, the potential liability of trustees is increased.

Trustees should ensure they have robust procedures in place to identify, assess, record and, where appropriate, notify data breaches. Trustees may also wish to revisit the protection from liability they obtain through the scheme and any liability insurance.

8. Contracts with data processors

The GDPR places direct legal obligations on data processors in relation to things like implementing appropriate data security measures and keeping a record of processing carried out on behalf of a data controller. Data processors are also required to ensure contracts with data controllers contain certain minimum provisions, such as a description of the scope, nature and purpose of processing.

Trustees should review and update their contracts with data processors to ensure there are appropriate provisions in relation to the data processor's new direct obligations and other relevant matters such as compliance, monitoring and reporting.

Liability and indemnity clauses in contracts should also be reviewed to ensure the risk allocation remains appropriate given that data processors now have direct legal obligations and given that the trustees and the data processors will have the same obligations in areas such as security. Data processors will be directly liable for breaches under the GDPR and so are more likely to seek indemnities from trustees in relation to data protection fines caused by the trustees.

If you would like further information on the developments referred to in this guide, our DP Toolkit or any other pensions or data protection legal issues, please get in touch with your usual contact in the Stephenson Harwood pensions team.

Mark Catchpole

Partner

T: +44 20 7809 2059
M: +44 7767 624 975
E: mark.catchpole@shlegal.com

Philip Goodchild

Partner

T: +44 20 7809 2166
M: +44 7825 384 004
E: philip.goodchild@shlegal.com

Graham Wrightson

Partner

T: +44 20 7809 2557
M: +44 7826 945 534
E: graham.wrightson@shlegal.com

Alex Rush

Senior associate

T: +44 20 7809 2187
M: +44 7711 347 524
E: alexander.rush@shlegal.com

Naeem Noor

Senior associate

T: +44 20 7809 2092
M: +44 7785 464 458
E: naeem.noor@shlegal.com

Dan Bowman

Consultant

T: +44 20 7809 2556
M: +44 7824 814 430
E: daniel.bowman@shlegal.com

www.shlegal.com

STEPHENSON HARWOOD

BD234-GDPR-0917