ALLEN & OVERY

Project planning for GDPR compliance: UK pension schemes

September 2017

GDPR:
What's new for pension scheme trustees?

The core data processing principles under the General Data Protection Regulation (the **GDPR**) will be familiar to trustees. As data controllers, you must be able to demonstrate that effective policies and procedures are in place to ensure that personal data are:

– processed lawfully, fairly and transparently;

– collected for a specified and lawful purpose;

– adequate, relevant and limited to what is necessary;

– accurate and up to date;

– not kept longer than necessary; and

– processed with appropriate technical and organisational measures in place to ensure security.

Beyond this familiar territory, though, GDPR preparation will be a significant issue for pension schemes, requiring a wide-ranging review of data protection issues and practices. Standard processes, contracts with administrators and other data processors, and member communications will all need to be updated.

Although it's unlikely that private sector pension schemes would normally be required to appoint a Data Protection Officer, as a matter of good practice you should designate someone to take responsibility for data protection compliance (without taking on the formal GDPR obligations of a Data Protection Officer) and build this into your governance arrangements.

Time is now relatively short, since the GDPR will take effect from 25 May 2018. Our project plan will help you to identify focus areas for the months ahead and prioritise actions to achieve compliance in good time.

Getting started: data inventory mapping and data flows 1

An early step in planning for, and achieving, GDPR compliance is to map your current data inventory and data flows. What data do you hold, where did it come from, and with whom do you share it? Administrators will be a key focus of scheme processing activity and data flows, but you should also consider communications teams, medical officers, actuaries, lawyers and other advisers, as well as any delegates and sub-contractors, as part of your data mapping exercise.

Data mapping is an important foundation for GDPR preparation: it will enable the GDPR requirements to be mapped to processing activities, to ensure compliance; and will help you begin to satisfy the requirement under the GDPR to maintain records of processing activities, as explained further below. It is also key to enabling compliance with a number of other requirements of the GDPR (such as responding to data subject access requests).

The GDPR includes a requirement for data controllers to undertake a privacy impact assessment (**PIA**) in some circumstances where there is a higher risk to the rights and freedoms of data subjects. Further guidance is expected in this area, but particular examples where a PIA may be required include situations where new technologies are being adopted, automated processing (profiling) is being undertaken, or sensitive data are being processed on a large scale. We would not normally expect these circumstances to apply on a straightforward change of pension scheme administrator, or to standard pension scheme processing, but trustees should note the requirement and seek further advice where necessary, as well as considering whether it would be appropriate to undertake a PIA in advance of a specific event, even if it is not mandatory.

Record keeping and accountability

2

The requirement to register data processing activities with the Information Commissioner's Office (**ICO**) will be eliminated under the GDPR. Data controllers will be required instead to maintain a written record of the processing activities for which they are responsible; the ICO may ask to inspect this from time to time. You must record all of the following information:

– the name and contact details of the controller (and any joint controller);

– the purposes of the processing;

– a description of the categories of data subjects and of the categories of personal data;

– the categories of recipient to whom the personal data have been or will be disclosed;

– where applicable, transfers of personal data to a third country or an international organisation, and the documentation of suitable safeguards;

– any envisaged time limits for erasure of the different categories of data (generally, trustees will need to hold data for long periods, even after a member leaves the scheme or dies, in case of potential challenges – this is normal practice in pension schemes, but you should record your reasons); and

– a general description of the technical and organisational security measures that are in place to ensure data security.

As well as maintaining mandatory records, most organisations are also building up more formal documented policy and control frameworks (where they do not already exist), with a view to demonstrating compliance to the ICO when required.

Data protection by design and by default is an express requirement under the GDPR – so, in conjunction with implementing policy and control frameworks and creating records of processing, consider whether you can minimise scheme data in terms of collection, retention or processing. For example, as well as eliminating the systematic collection or retention of any unnecessary data, it may often be possible to remove identifying details from queries sent to advisers, where these have no bearing on the outcome of the query.

Basis for lawful processing

3

As part of the data mapping and inventory exercise, data controllers should review the legal basis on which they rely in relation to each type of data processing they undertake. The basis may need to change under the GDPR, which could have implications for your fair processing notices. Lawful grounds for processing include:

– **Consent**: Under the GDPR, consent to data processing must be unbundled (ie consent must be given individually for each purpose of processing), distinguished from other matters (ie it cannot be buried within lengthy terms and conditions or privacy notices) and genuine (ie there must be a genuine choice offered, rather than a 'take it or leave it' approach). There are other hurdles too, so most schemes are unlikely to rely on consent as a basis for routine pension scheme processing.

– **Compliance with a legal obligation**: The need to comply with legal obligations may provide a basis for trustee data processing in many circumstances (although it is important to check who is the subject of the legal obligation – for example, in relation to auto-enrolment, this is generally the employer rather than the trustees).

– **Legitimate interests**: Data processing may be valid where it is necessary for the purposes of legitimate interests pursued by the data controller or another third party. Subject to further ICO guidance (expected later this year), we anticipate that this will be a potentially useful ground for trustee data processing that falls outside the 'legal obligation' category, at least for private sector schemes (the GDPR recitals suggest that it may not be appropriate for public sector schemes).

For some types of data – for example, in relation to health or sexual orientation – explicit consent is generally required. This means consent must have an additional degree of formality attached (such as a signature or tick box) and cannot be implied. This could be relevant in relation to ill-health or (in some cases) death benefit processes – do your documents and procedures comply with these requirements?

The legal basis on which you rely for data processing needs to be specified in fair processing notices and the information you provide in response to subject access requests. Some individuals' rights will be modified depending on the legal basis you are using – for example, the right to data deletion will be especially relevant if you are relying on consent as the basis for processing.

Fair processing notices

4

Review the information you currently provide to members about data privacy and processing, so that you are able to plan any necessary changes to your current fair processing/privacy notices. The GDPR requires data controllers to provide information to data subjects, including the following:

– the identity and contact details of the data controller;

– the purpose and legal basis for processing data;

– the recipient(s) or categories of recipient;

– how long data will be retained (or the criteria used to determine that period);

– their rights as data subjects, including the right to complain if they are dissatisfied with how their data are handled; and

– transfer outside the EEA and the terms of transfer.

We expect that all schemes will need to update and reissue their fair processing notices. There is no transitional arrangement for existing notices that do not meet the new requirements.

The GDPR requires notices to be provided to every member, which may be problematic where schemes have gaps in contact details in relation to deferred members (although the GDPR provides some leeway where disproportionate efforts would be required).

Arrangements with third parties

5

As under the existing law, you are required to have in place a written agreement with any third party data processors undertaking data processing activities on your behalf. The GDPR expands the provisions that must be included in that contract. Under the GDPR, you must ensure that the processor:

– processes data only on your instructions and does not use it for any other purpose;

– ensures confidentiality;

– ensures appropriate technical and organisational measures for data security;

– assists with subject access requests;

– ensures data are deleted or returned on termination of the contract;

– does not transfer data abroad without ensuring appropriate safeguards (as agreed in the contract);

– assists with compliance obligations;

– passes on obligations to delegates; and

– agrees an appropriate allocation of risk/liability for breaches.

Contracts must also include appropriate compliance, reporting, liability and monitoring provisions. The process of renegotiating these provisions of existing agreements will take time, so it makes sense to start this process as soon as possible (and ideally to pick up amendments as part of the usual renewal cycle where possible). Remember that your data processors may also be seeking changes, since they will have direct GDPR obligations and will want to minimise their liability in light of the greater potential sanctions that may be imposed under the GDPR.

It's worth noting that some actuaries have registered as data controllers – if your scheme actuary is also a data controller alongside the trustees, changes may well be advisable to their terms of engagement to reflect this status and to clarify the parties' respective roles and responsibilities, for example in relation to the provision of information to members.

Members' rights

6

Check your procedures (or your administrator's procedures) for dealing with subject access requests (that is, the data subject's right to access the personal data collected concerning him/her) or requests to erase their data. You must respond to requests without undue delay and at the latest within one month; additional information must be provided, and grounds for refusal will change. You must have appropriate measures in place to provide data subjects with information relating to the processing in a concise, transparent, intelligible and easily accessible form.

The GDPR gives individuals some new rights – for example, individuals will gain the right to data portability in some circumstances. Where the right exists, you must be able to provide members with that data electronically and in a commonly-used format.

Ensure that processes are updated to meet the new deadlines and requirements.

Personal data breach notification

7

Data controllers are required under the GDPR to notify breaches to the relevant authority (in the UK, the ICO) without undue delay and (where feasible) within 72 hours of awareness, except where the breach is unlikely to result in a risk to the rights and freedoms of individuals. In addition, if the breach creates a high risk for individuals (for example, if it leaves them open to discrimination, fraud or financial loss) then the data controller must notify affected individuals without undue delay.

You will need a robust process for detecting, investigating, recording and, where relevant, notifying personal data breaches. This should include a communications strategy for affected individuals and other stakeholders.

Establish a framework for accountability, including training for trustees and internal administrators and safeguards to minimise and secure data processing. You also need to ensure that there are clear requirements and processes in place for your data processors to inform you of any breach.

Taking reasonable steps in advance to reduce the incidence and impact of data breaches will also help to mitigate the risk of severe penalties. For example, data encryption may enable you to demonstrate, in the event of breach, that there is no risk to the rights and freedoms of individuals.

Transferring data outside the EEA

8

Cross-border data transfers outside the European Economic Area (the **EEA**) will continue to be prohibited unless the third country ensures adequate protection or other conditions are met. There are various ways of ensuring protection: you can use standard model clauses for international data transfer in your agreements with processors, or 'binding corporate rules' which guarantee data safeguards on intra-group transfers. You can also seek to mitigate the risk by moving servers to the EEA or anonymising data pre-transfer.

Check with your data processors whether they transfer scheme data outside the EEA and if so, on what basis. Ensure that appropriate arrangements are in place to legitimise ongoing or future cross-border data transfers. The UK's own adequacy status could be affected by the UK's exit from the EU; keep a watching brief on future developments in this area.

Cybersecurity

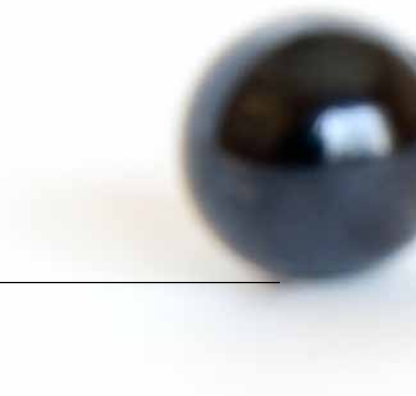
9

You may already have undertaken a separate review of your cybersecurity practices, but it's important to make the connection with GDPR compliance and the requirement to have technical and organisational measures in place to ensure data security. For example:

– When looking at data flows, the simplest way to improve data security is to minimise transmission: do trustees or their advisers really need identifying member details, or could information be anonymised to reduce the potential consequences of any data loss? Any personal data which are transferred should be encrypted.

– When reviewing contracts with third-party administrators and other providers, check that they have policies and processes in place to prevent cyber breaches. The contract should also include a clear allocation of cybersecurity risks and governance responsibilities, from minimum requirements, monitoring and reporting, to incident management, liability and compensation in the event of breach.

For more tips, see our separate cybersecurity **guide** and **checklist***.



*Also available at www.allenovery.com/pensionsindispute

A note on sanctions

The ICO will be able to impose fines of up to the higher of 4% of annual worldwide turnover and EUR20m for certain breaches of the GDPR, for example breach of the basic principles for processing. It's currently unclear how this will apply to pension scheme trustees, since the percentage fine applies to an 'undertaking', as described in the Treaty on the Functioning of the European Union. This is interpreted by assessing the degree of control by entities within a corporate group. Further guidance is awaited, but there is at least a potential for fines for breach in relation to an occupational pension scheme to be assessed on a percentage basis, based on the turnover of the wider group.

When deciding whether to impose a fine, the ICO will take into account factors such as:

– the nature, gravity and duration of the infringement;

– the purpose of the processing concerned;

– the number of data subjects affected and the level of damage suffered by them;

– the intentional or negligent character of the infringement;

– action taken to mitigate damage suffered by data subjects; and

– the manner in which the data breach became known to the ICO.

No organisation can eliminate all risk of data breaches, but thorough, timely and well-documented GDPR preparations will help not only to mitigate the risk of breaches, but to minimise the penalties if the worst happens and a breach does occur.

Key Contacts

Maria Stimpson
Partner
Tel +44 20 3088 3665
maria.stimpson@allenovery.com

Däna Burstow
Partner
Tel +44 20 3088 3644
dana.burstow@allenovery.com

Neil Bowden
Partner
Tel +44 20 3088 3431
neil.bowden@allenovery.com

Jane Higgins
Partner
Tel +44 20 3088 3161
jane.higgins@allenovery.com

Jane Finlayson-Brown
Partner
Tel +44 20 3088 3384
jane.finlayson-brown@allenovery.com

Nigel Parker
Partner
Tel +44 20 3088 3136
nigel.parker@allenovery.com

Jessica Kerslake
Counsel
Tel +44 20 3088 4710
jessica.kerslake@allenovery.com

Andy Cork
Counsel
Tel +44 20 3088 4623
andy.cork@allenovery.com

Helen Powell
PSL Counsel
Tel +44 20 3088 4827
helen.powell@allenovery.com

High-level GDPR project plan

Area	Immediate – start now	Q4 2017 to 24 May 2018	Ongoing actions
Foundations	Consider trustee training needs: do trustees understand the need for action? Review resourcing (time and budget) for GDPR compliance activities. Build time into your business plan/contact processors and advisers to agree deadlines. Confirm whether the scheme needs to appoint a DPO and, if not, consider allocating responsibility for scheme GDPR compliance. Liaise with the sponsor's data protection or compliance officer as appropriate.	Record all policy documentation as part of your privacy framework assessment. See '**Record keeping and accountability**'. 2 Review ways to implement 'privacy by design', eg by minimising data collection and by anonymising data before sharing it. See '**Record keeping and accountability**'. 2	Monitor and report on privacy compliance. Consider the need for a privacy impact assessment if undertaking high risk processing in future. See '**Getting started**'. 1
Data inventory and mapping	Analyse current data processing activities: what data do you hold, where did it come from, and with whom do you share it? See '**Getting started**'. 1	Ensure trustees and administrators understand your privacy by design policy and operate according to it.	
		Review basis for any future cross-border processing See '**Transferring data outside the EEA**'. 8 Update arrangements and ensure processor contracts include appropriate provisions.	Monitor the implications of Brexit for cross-border processing. See '**Transferring data outside the EEA**'. 8
Lawful processing	Review current processing activities; consider the purpose and lawful grounds for each type of processing, including the nature of the trustees' 'legitimate interest' where relevant. See '**Basis for lawful processing**'. 3 Consider sensitive personal (eg health-related) data: would current processes meet the explicit consent requirement? See '**Basis for lawful processing**'. 3	Review and update fair processing notices (and, where applicable, consents) in line with GDPR requirements. See '**Fair processing notices**'. 4 Issue to members before 25 May 2018. Update processes where sensitive personal data are relevant, eg ill-health applications/death benefit processes, to ensure you obtain consent in line with the GDPR and record that it was validly given.	Include ongoing reminders about data protection/fair processing in member newsletters/ benefit statements etc.
Administration /processor contracts	Identify all data processors and review current contracts for key terms. See '**Arrangements with third parties**'. 5 Renegotiate contracts as required (prioritise key parties such as administrators – see also below).		Monitor processor compliance in line with contract.
Specific processes	Review current processes, eg for breach notification and subject access requests. Are changes required to meet new deadlines? See '**Members' rights**' 6 and '**Personal data breach notification**'. 7	Update agreements/implement new processes for breach detection and reporting. Ensure that these are robust, documented and well understood, including an action plan for communications where required. See '**Personal data breach notification**'. 7	Consider carrying out data breach fire drill as a training exercise.
		Review safeguards to ensure that admin procedures minimise the incidence and impact of data breaches. See also '**Cybersecurity**'. 9	
Risk review	Conduct risk review of overall data protection arrangements.	Mitigate risks/update risk register as appropriate.	Monitor and review in light of future developments.

Blue text indicates areas where changes may be required to current arrangements with administrators and other processors. It is important to start this work as soon as possible. See '**Arrangements with third parties**'. 5

● Section number

FOR MORE INFORMATION, PLEASE CONTACT:

London

Allen & Overy LLP
One Bishops Square
London
E1 6AD
United Kingdom

Tel +44 20 3088 0000
Fax +44 20 3088 0088

GLOBAL PRESENCE

Allen & Overy is an international legal practice with approximately 5,400 people, including some 554 partners, working in 44 offices worldwide. Allen & Overy LLP or an affiliated undertaking has an office in each of:

Abu Dhabi
Amsterdam
Antwerp
Bangkok
Barcelona
Beijing
Belfast
Bratislava
Brussels
Bucharest (associated office)
Budapest
Casablanca
Doha
Dubai
Düsseldorf
Frankfurt
Hamburg
Hanoi
Ho Chi Minh City
Hong Kong
Istanbul
Jakarta (associated office)
Johannesburg
London
Luxembourg
Madrid
Milan
Moscow
Munich
New York
Paris
Perth
Prague
Riyadh (cooperation office)
Rome
São Paulo
Seoul
Shanghai
Singapore
Sydney
Tokyo
Warsaw
Washington, D.C.
Yangon

Allen & Overy means Allen & Overy LLP and/or its affiliated undertakings. The term **partner** is used to refer to a member of Allen & Overy LLP or an employee or consultant with equivalent standing and qualifications or an individual with equivalent status in one of Allen & Overy LLP's affiliated undertakings.