ALLEN & OVERY

Data protection and UK pension schemes

Practical issues and future developments

2016

Data protection is changing

Most pension scheme trustees will be familiar with the basics of data protection – but how do they apply in practice, in a landscape where data risks have changed radically? And what difference will new rules, in the form of the General Data Protection Regulation, make when they come into effect from 25 May 2018?

This briefing provides a refresher on the basics of data protection, highlighting practical issues for pension schemes under the current law, as well as signposting key areas where trustees need to start preparing now for future change.

© Allen & Overy LLP 2016

A refresher on the basics

Pension schemes run on personal data – that includes everything from a member's name, address and date of birth details to their salary and other financial information. Some of that personal data will be sensitive (for example, information about a member's physical and mental health).

By virtue of their role in handling members' personal data, trustees are data controllers under the Data Protection Act 1998 (the **DPA**). Typically, data processing is carried out on trustees' behalf by internal or external administrators, but trustees should also consider a wider range of service providers – for example, communications teams, medical officers, investment consultants, actuaries and lawyers could also be relevant. Legal responsibility for DPA compliance falls on data controllers rather than data processors.

The DPA sets out eight data protection principles which govern the way that personal data is obtained, stored, used and shared; it also sets out the conditions subject to which personal data may be processed. The diagram on the next two pages highlights issues which are particularly relevant for pension scheme trustees.

Jargon buster

Data includes any information recorded as part of a relevant filing system (whether electronic or paper-based) or other accessible record and which is or can be processed automatically.

Data controller means a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which, any personal data are, or are to be, processed.

Data processor means any person (other than an employee of the data controller) who processes the data on behalf of the data controller.

ICO means the Information Commissioner's Office, the UK data protection regulator.

Personal data means data which relate to a living individual who can be identified from that data or from that data and other information which is in, or is likely to come into, the possession of the data controller.

Processing means obtaining, recording or holding information or data or carrying out any operation involving data, including organising, altering, retrieving, consulting or using it. It also includes disclosing the data and ultimately erasing or destroying it.

Sensitive personal data includes information about a member's physical and mental health. It does not encompass simple financial information. Additional restrictions apply to sensitive personal data.

Practical reminders for pension scheme trustees

Data controllers must follow the data protection principles:

The data protection principles	
Personal data must be processed fairly and lawfully (including meeting appropriate conditions – see facing page).	Have you reviewed your fair processing notice recently? Is the language up-to-date? Does it cover all purposes for processing and all potential data recipients? This can be an issue, for example, on DB transfer exercises. Traditionally, this notice was frequently given alongside the membership application form, but with the roll-out of auto-enrolment, application processes have in many cases become redundant. Is information given in the scheme booklet, or in member newsletters? Do all members receive it?
Ensure personal data are obtained and processed for specified and lawful purposes and are not processed in any manner incompatible with those purposes.	
Ensure personal data are adequate, relevant and not excessive in relation to processing purpose.	Ensure that you do not hold irrelevant information, by arranging for periodic data audits. Forms and questionnaires should only require information which is relevant to their purpose.
Ensure personal data are accurate and kept up-to-date.	This is the foundation for much wider trustee responsibilities – for example, implementing the Pensions Regulator's guidance on improving data quality, and the reconciliation of data underlying guaranteed minimum pensions. Do you know your scheme's conditional data score? Are you still taking action to improve it?
Keep personal data no longer than is necessary.	Statutory record-keeping requirements often set minimum periods for keeping data, but these may not be long enough to enable trustees to respond to member queries or complaints, potentially decades into the future. You need to consider on a case-by-case basis whether particular records still need to be retained for the purposes of the scheme.
Process personal data in accordance with the rights of data subjects.	
Appropriate technical and organisational measures must be in place to protect against unauthorised or unlawful processing, and against accidental loss or destruction of personal data.	This will typically require contracts to be put in place with processors and data importers. See pages 6 and 7.
Personal data should not be transferred to a jurisdiction that does not offer an adequate level of data protection.	

© Allen & Overy LLP 2016

Personal data may not be processed unless one or more of the following conditions is met*:

The individual has consented. Consent must be freely given, specific and informed.	Obtaining member consent has generally been the most straightforward way for trustees to comply with the first data protection principle. Traditionally, members consented by signing a response to a fair processing notice. Again, auto-enrolment complicates matters, since trustees cannot require workers to give their consent to data processing as a condition of membership. Other conditions must be considered where consent is not available.
Processing is necessary for the performance of a contract to which the individual is a party or for the taking of steps at the request of the data subject with a view to entering into a contract.	
Processing is necessary for compliance with a legal obligation (other than an obligation imposed by contract) to which the data controller is subject.	For the purposes of enrolment and re-enrolment, the 'statutory compliance' condition will protect trustees. However, in the normal lifecycle of a scheme, processing will extend to activities which are not required by legislation – for example, sending out scheme newsletters or other information.
Processing is necessary for the purposes of the legitimate interests of the data controller or the third party to whom the data is disclosed (this must be balanced against the individual's legitimate interests).	Trustees may be able to validate processing on the grounds that it is within their legitimate interests as data controllers – for example, to assess the membership profile in order to make decisions about DC investment options, or to send non-mandatory information to members.

Sensitive personal data may not be processed without the individual's explicit consent.

*The DPA sets out further conditions for processing, but these are the most relevant in the pension scheme context.

'Appropriate technical and organisational measures' for data security

With increasing awareness of cyber risks, ensuring data security is a very hot topic. Data controllers must put appropriate technical and organisational measures in place to protect against unauthorised or unlawful processing, and against accidental loss or destruction of personal data. Breach of the data security principle is the most common trigger for enforcement action being taken by the ICO.

The actual measures to be taken will vary depending on the sensitivity of the data, technological developments and implementation costs, but you should ensure compliance both by the scheme and by any third party data processors. You should also review and monitor compliance regularly.

Further help

For more information, please get in touch with any of our experts listed at the back of this briefing, or see our separate guide 'Cybersecurity and pension schemes'.

Your data processing arrangements

The DPA lays down specific requirements for the contract between a data controller and data processor. The agreement must:

– be in writing;

– include a requirement that the processor acts only on the controller's instructions; and

– require the processor to comply with data security obligations equivalent to those applying to the controller.

You should review existing data processing arrangements to ensure that they include these requirements and that reporting and monitoring arrangements for data security are satisfactory to the trustees. If cross-border data transfer is envisaged, then appropriate provisions should be included.

The contract should also set out how subject access requests and other communications from members are to be dealt with (including response times) and should cover the termination of the contract, to ensure a smooth handover to new administrators and appropriate protection for all data during that process.

The requirement for a written contract could also apply to actuaries, payroll agents and members' employers if they undertake any processing on your behalf.

© Allen & Overy LLP 2016

Transferring data outside the EEA

Cross-border data transfer is another hot topic. In brief, cross-border data transfers outside the European Economic Area (EEA) are prohibited unless the third country ensures adequate protection or other conditions are met.

There are various ways of ensuring protection: for example, you could 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 could seek to mitigate the risk by moving servers to the EEA or anonymising data pre-transfer. The first step is to audit your current practices – check with your data processors whether data is being transferred outside the EEA and if so, on what basis.

In respect of transfers from the EEA to the U.S., 'Safe Harbor' arrangements previously facilitated transfers by deeming entities registered under the EU-U.S. Safe Harbor to provide an adequate level of protection. This ceased to apply following the *Schrems* case, in which the Court of Justice of the European Union declared Safe Harbor invalid. This led to the development of the EU-U.S. Privacy Shield Framework as a replacement for Safe Harbor, which has been approved by the European Commission as adequate to enable data transfers under EU law.

Further help

If you need further help in relation to cross-border transfers, please get in touch with any of our experts listed at the back of this briefing.

Enforcement and penalties

The ICO is responsible for enforcement in this area, and has the power to impose fines of up to GBP500,000 for serious breaches of the DPA. The penalties apply to data controllers who seriously contravene the data protection principles in a way which is likely to cause substantial damage or substantial distress and either:

– the contravention was deliberate; or

– the data controller knew or ought to have known that there was a risk of contravention, and that such contravention would be likely to cause substantial damage or substantial distress, but failed to take reasonable steps to prevent it.

Even if a data protection breach is committed by a third party data processor, the offence is committed by, and the penalty attaches to, the data controller – so your contracts with data processors should take account of this and include appropriate protection.

The ICO will also take into account the nature of the personal data involved and the number of individuals affected or potentially affected by the contravention. It will also consider whether the data controller has taken reasonable steps to prevent a contravention, such as maintaining appropriate policies and audit arrangements to make sure that all parties comply with the required security measures.

Individuals may also claim for compensation if they have suffered damage or distress as a result of any failure by the trustees to comply with the DPA.

What's coming next: the GDPR

The General Data Protection Regulation (GDPR) will apply in EU Member States from 25 May 2018. The GDPR will introduce a number of changes to current data protection rights and duties, and the ICO is due to produce guidance in the coming months about what this will look like in practice.

A word about Brexit:

The GDPR will be directly applicable in Member States from 25 May 2018 and needs no additional legislation to give it effect. Based on the current Brexit timetable, it will therefore apply for a period before the UK's formal exit from the EU. On a practical level, it is expected that the UK would adopt a post-exit data protection law in broadly similar terms to the GDPR, to ensure that the UK is considered 'adequate' for the purposes of data exports from the EU; this may also be a specific requirement of the UK's post-exit status. This has recently been confirmed by the UK government. For multinationals, the drivers for adopting GDPR-compliant policies and systems apply regardless of Brexit.

© Allen & Overy LLP 2016

What difference will the GDPR make to trustees?

The following issues are of particular relevance in the pension scheme context:

Consent requirements will change

Where consent is relied on as a condition for processing, the GDPR enhances the current consent requirements by making valid consent subject to additional conditions. For example, consent can be withdrawn at any time; the GDPR requires data controllers to inform data subjects of this right and ensure that it is as easy for them to withdraw consent as to give it. There is a raft of other hurdles too. Particularly in the context of auto-enrolment, it is likely to become difficult to rely on consent as a basis for routine pension scheme processing, so you will need to look towards a different legal basis such as statutory compliance, or legitimate interests.

The recitals to the GDPR suggest that a 'relevant and appropriate relationship' between data subject and data controller (such as the individual being in the service of the controller) could be sufficient to establish a 'legitimate interests' basis for processing – subject to further ICO guidance, this is a potentially useful ground for trustees to use, at least in the private sector (the GDPR recitals suggest that that this would not be appropriate for the public sector).

Information requirements will increase

Data controllers will be required to provide additional information to data subjects, including details of their legal basis for processing data, how long data will be retained, and that individuals can complain to the ICO if they are dissatisfied with how their data is handled.

This information must be provided in concise, easy to understand and clear language. Notices will need to be updated. There is no transitional arrangement for existing notices that do not meet the new requirements.

Individuals' rights will change

Individuals will gain some new rights – for example, the right to have their data deleted – which may have only limited impact in the pension scheme context. However, subject access rights will also change – the time period for compliance will reduce from 40 days to one month; additional information must be provided, and grounds for refusal will change. Individuals will also gain the right to data portability – to have their data provided electronically in a commonly-used format.

Breach notifications will be a major compliance issue

Data controllers are required under the GDPR to notify breaches to the relevant authority 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. Failure to notify carries its own sanction (in addition to any sanction for the data breach itself). A penalty of up to EUR10 million or, for an undertaking, up to 2% of the annual worldwide turnover for the preceding financial year could be imposed (whether the failure is intentional or negligent).

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. Data subjects can also claim compensation for both material and immaterial damage – immaterial damage could include, for example, non-financial elements such as distress or inconvenience resulting from a breach of the GDPR.

You will need a robust process for identifying, recording and, where relevant, notifying personal data breaches This should include a communications strategy for affected individuals and other stakeholders. The provisions also underline the crucial importance of encrypting data so that, in the event of breach, you can show that there is no risk to the rights and freedoms of individuals.

An increased focus on accountability

Data controllers will be required to:

– maintain records of all processing activities for which they are responsible;

– conduct data protection impact assessments for risky processing (for example where a new technology is being deployed);

– demonstrate that effective policies and procedures are in place to comply with data protection principles;

– implement data protection by design and by default; and

– appoint a data protection officer if required, or designate responsibility for compliance to an appropriate person.

Data processors will have obligations too

Data processors will have direct obligations, for example in relation to implementing data security measures and assisting the data controller on breach notifications and subject access requests.

You will need to review and update relevant procedures and the provisions of your service level agreements to ensure that appropriate data security requirements are included and that liability is appropriately allocated. Where changes to service standards are required, you may need to consider where the burden of any costs will fall under your current agreements.

© Allen & Overy LLP 2016

Sanctions may be much greater

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.

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 it's worth noting that there is a rebuttable presumption that a 'dominant influence' exists between parent and subsidiary/associate undertakings (or where the controlling undertaking has power to have personal data protection rules implemented). This means that 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.

The recitals to the GDPR also state that where a fine is imposed on an entity which is not an 'undertaking' then the economic situation of the potential target should be taken into account in determining the appropriate amount (up to the EUR20m cap), and again it is currently unclear whether the wider group's turnover would be considered relevant.

Further guidance is needed in these areas, and we hope this will also clarify whether the assessment of penalties depends to any extent on the structure of the trustee (for example, whether it is a corporate subsidiary or non-incorporated trustee body).

How can trustees start preparing for the GDPR?

Carry out an information audit

What data do you hold, where did it come from, and with whom do you share it? You will need to know this to assess what other actions are required. It's also worth considering whether all the data collected is essential: the GDPR emphasises data protection 'by design and by default', which means minimising data collected so far as possible.

Consent

How do you currently seek and obtain consent to data processing? Are changes to that process required? Consent must be a positive indication – it cannot be inferred, for example from failure to respond, or pre-ticked boxes. You should ensure that consent documentation is up-to-date and that you have an audit trail recording consent, where this is the legal basis on which you rely.

Legal basis for processing

What legal basis do you rely on, in relation to each type of data processing you undertake?

Have you documented this and considered the impact of future changes – for example, providing this information in privacy notices and 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.

Privacy/fair processing notices

Review the information you currently provide, and how you provide it, so that you are able to plan any necessary changes – for example explaining the legal basis on which you will process data, how long you will retain it, and the mechanism for members to complain to the ICO.

Subject access requests

Check your procedures (or your administrator's procedures) for dealing with subject access requests and other requests from individuals – timescales will change and additional information will be required.

© Allen & Overy LLP 2016

Third party contracts

Are changes required to your current agreements with data processors? Service level agreements and contracts with other data processors will need to be reviewed to ensure that mandatory provisions are included, as well as appropriate compliance, reporting, liability and monitoring provisions.

If a legal review is required, ensure that you get this in plenty of time before the implementation deadline – and remember that if you are currently negotiating any administration services or other relevant agreements (for example, in relation to liability management exercises) which will last beyond May 2018, these should incorporate GDPR-compliant provisions.

Preparing for data breaches

Put procedures in place to ensure you can detect, report and investigate personal data breaches quickly (particularly where the breach may lead to financial loss for the individual). Failure to report a breach when required is itself a breach of the GDPR.

Who is responsible for data protection compliance in your organisation? Establish a framework for accountability, including staff training and safeguards to minimise and secure data processing.

Taking reasonable steps in advance to reduce the incidence and impact of data breaches will also help to mitigate the risk of severe penalties.

Risk register

Update your risk register in light of current and future developments in this area.

Key Contacts

Pensions

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

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

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

"Allen & Overy's 'first-rate' team 'consistently delivers well-presented and focused advice that inspires confidence in its clients'."

Legal 500 (Pensions) November 2016

© Allen & Overy LLP 2016

Data protection

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

David Smith
Peerpoint Consultant
Tel +44 20 3088 6842
david.a.smith@allenovery.com

Charlotte Mullarkey
Counsel
Tel +44 20 3088 2404
charlotte.mullarkey@allenovery.com

"They are commercial, responsive, innovative and impressive to work with. They took the time to get to know our business and the results have been fantastic."

Chambers UK (Data Protection) 2015

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 5,200 people, including some 530 partners, working in 44 offices worldwide. Allen & Overy LLP or an affiliated undertaking has an office in each of:

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

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.

This document is for guidance only and does not constitute definitive advice.
© Allen & Overy LLP 2016 | CS1610_CDD-46522_ADD-63671