Data protection and cyber security – issues for pension schemes

2 November 2016
Agenda

• Cyber security and data protection
  – What’s the current situation?
  – What may change?

• Putting it into practice – a pension scheme case study

• Practical takeaways – what should trustees be doing?
Cyber security and data protection
Cyber security and data protection

- Members' names and addresses
- Bank account details for pensioners
- Death benefit nomination forms
- Medical reports
- Marital status
- Member's age
- Information about pay
- Information about investment performance and strategy
- Actuarial assumptions
Cyber security and data protection

Personal Data

Sensitive Personal Data

Data
## Cyber security and data protection

<table>
<thead>
<tr>
<th>Data Protection Category</th>
<th>Data</th>
<th>Personal Data</th>
<th>Sensitive Personal Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Members' names and addresses</td>
<td>√</td>
<td>√</td>
<td></td>
</tr>
<tr>
<td>Bank account details for pensioners</td>
<td>√</td>
<td>√</td>
<td></td>
</tr>
<tr>
<td>Death benefit nomination forms</td>
<td>√</td>
<td>√</td>
<td>(✓)</td>
</tr>
<tr>
<td>Medical reports</td>
<td>√</td>
<td>√</td>
<td>✓</td>
</tr>
<tr>
<td>Actuarial assumptions</td>
<td>√</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Information about investment performance and strategy</td>
<td>√</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Information about pay</td>
<td>√</td>
<td>√</td>
<td></td>
</tr>
<tr>
<td>Member's age</td>
<td>√</td>
<td>√</td>
<td></td>
</tr>
<tr>
<td>Marital/civil partnership status</td>
<td>√</td>
<td>√</td>
<td>(✓)</td>
</tr>
</tbody>
</table>
Data protection principles

- Fair and lawful processing
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Security
- Rights of data subjects
- Data export restriction
- Accountability (new under GDPR)
How does cyber security fit in?

- Cyber security is concerned with protecting IT systems against attack.
- Risks may be to personal data, to non-personal confidential information, or to the availability of the systems themselves.
Cyber security

• ActionFraud estimate that 70% of fraud is cyber-enabled
• 65% of large businesses detected a cyber security breach or attack in the past year; 25% of these experience at least one a month
• Average cost of a breach to large businesses is £36,500
• Malware/viruses the most common type of breach
• In one survey 50% of organisations attributed the cause of their worst breach of the year to inadvertent human error
Cyber security

• Trustees are responsible for protecting information
• Should be part of internal control processes
• Remember suppliers are a critical part of the security picture
• Potential liability for breaches, including maladministration claims to Pensions Ombudsman and fines by the ICO
Case study
The ABC (UK) Pension Plan

Employers
• Sponsoring employer: ABC (UK) Limited
• Part of global corporate group producing abacuses and other educational toys

Benefits
• Defined benefit (DB) section closed to new members
• Defined contribution (DC) section open and used for auto-enrolment
• Death in service lump sum
• Ill-health pensions
The ABC Pension Plan: two members

Anita
• Joined scheme in 1995
• Member of DB section

Bart
• Joined ABC (UK) Limited in 2016
• Auto-enrolled into DC section
Scene 1
Joining a scheme – how data is collected

• **Anita**
  – Joined in 1995 by completing an application form
  – Information included her name, address, sex, date of birth and spouse/partner's name
  – Application form contained no reference to what the information may be used for

• **Bart**
  – Joined automatically (auto-enrolled) on starting employment
  – No application form completed
  – Employer passed member data to trustees: age, sex, address, salary
Joining a scheme – what needs to be done?

• **What type of data is it?**
  – Personal?
  – Sensitive?

• **What are the issues?**
  – Key data protection principle is that data must be processed *fairly and lawfully*
  – To be processed "fairly and lawfully":
    – Must be able to satisfy one of the specified "grounds" for processing eg consent, necessary for legitimate interests, necessary for performance of a legal obligation
    – Must provide information to individuals about how the information will be used
Joining a scheme – what needs to be done?

• **What must trustees do?**
  – Trustees need to decide on the grounds for processing:
    – Legitimate interest – personal data?
    – Consent – sensitive personal data?
  – Trustees need to "make available" to Anita and Bart the following:
    – Who controls their data
    – What it will be used for (NB don't have to set out obvious uses)
    – Who it may be shared with
  – Trustees need to assess how use may have changed over time

• **Any changes?**
  – GDPR will require more detailed notices to members
Scene 2
Holding members' data – general

- Member data is held by EU-wide shared service centre in Madrid run by ABC (Europe) S.A.
- All pensions data held there
Holding members' data – general

• **What type of data is it?**
  – Personal?
  – Sensitive?

• **What are the issues?**
  – Trustees are outsourcing the processing to a third party (even though in employer's group)
  – Trustees remain responsible for the data, even where the failure is that of a service provider
  – Key data protection principle is "security" – special provisions apply where processing is outsourced
Holding members' data – general

• **What must trustees do?**
  – Carry out appropriate due diligence
  – Put in place a contract with ABC (Europe) S.A. that includes requirements that the S.A.:
    – Only processes the data on the trustees' instructions
    – Has appropriate technical and organisational security measures in place

• **Any changes?**
  – GDPR imposes more prescriptive contracting requirements
Scene 3 – liability management
Liability management

• ABC (UK) Ltd is conducting a review of its pension liabilities with a view to considering various liability management options

• Trustees are asked to supply detailed information about deferred members' benefits as this is not retained by the employer

• The data comprises: name, address, sex, date of birth and last known marital/civil partnership status, final pensionable salary and length of service
Liability management

• What type of data is it?
  – Personal?
  – Sensitive?

• What are the issues?
  – Trustees are being asked to share data
  – Key data principles:
    – Fairness: have members been told their data will be shared?
    – Purpose limitation: is this a specified purpose?
    – Legitimate grounds for processing: does this apply?
    – Data minimisation: could the data be anonymised/minimised?
Liability management

- **What must trustees do?**
  - Assess if they are able to pass member information to ABC (UK) Ltd
  - Review previous notices given
  - If not adequate – creative/pragmatic approach and consider data sharing agreement/NDA

- **Any changes?**
  - No!
Scene 4 – security breach
Security breach!

- Hackers gain access to the shared service centre's systems and steal pensioners' information
- The data comprises: NI numbers, addresses, DOBs, details of bank accounts to which pensions are paid
Security breach!

• What type of data is it?
  – Personal?
  – Sensitive?

• What are the issues?
  – Containing the breach, and understanding its cause and impact
  – Potential breach of data protection security principle
  – Potential liability to members (pensions ombudsman)
Security breach!

• **What must trustees do?**
  - Work with ABC (Europe) S.A to understand the breach and implications
  - Consider notification: ICO, members, other system users, law enforcement, insurers
  - Review the breach response handling processes
    - Do you have an incident response plan?
    - How often do you test your IRP?
    - Do you have a short list of vendors to provide technology services in the event of a breach?
    - Do you know which regulators you need to notify in the event of a breach?
    - Do you have a plan for communicating breaches to affected members? Will you offer identity theft or credit monitoring services?
Security breach!

• **Any changes?**
  – Notification will become mandatory: data protection authority and members impacted by the breach
  – Obligation to keep records of breaches
Scene 5 - outsourcing
The Trustees have decided they are not happy with the shared service centre.

Decided to appoint BenefitsRUs SA as administrator as it supplied the cheapest quotation – partly, it claims, as it uses IT services based in south Asia.
Outsourcing

• **What type of data is it?**
  – Personal?
  – Sensitive?

• **What are the issues?**
  – Trustees are deciding to outsource processing to unknown provider on basis of contract price
  – Trustees remain responsible for the data, even where the failure is that of a service provider
  – Key data protection principle is "security" – special provisions apply where processing is outsourced
  – Trustees are aware that the provider will process information outside the EU
  – Key data principle is data export restriction – additional provisions apply where data leaves the EU
Outsourcing

• **What must trustees do?**
  – Due diligence is essential
    – eg what security does the processor have in place?
    – eg how does the supply chain work? Do BenefitsRUs host the data themselves or are they using a third party?
  – Put in place an appropriate contract including the following:
    – contract obligations need to flow down to the vendor's own suppliers, as these are also processors for the trustees
    – European Commission standard contractual clauses on data export

• **Any changes?**
  – Under GDPR processors will have some direct liability
Scene 6 – ill-health
Ill health early retirement

- Anita has been off sick with back pain since July 2015 and has now applied for ill health early retirement (IHER)
- The HR department at ABC (UK) Ltd are sceptical about the severity of Anita's condition and set out their concerns in a memo to the Trustees, at the same time as passing on Anita's IHER application and copies of reports from her GP and pain specialist. The Trustees pass the information to an external occupational health specialist and ask for an opinion
Anita's application for ill health early retirement

- **What type of data is it?**
  - Personal?
  - Sensitive?

- **What are the issues?**
  - Express consent is needed for processing
  - Anita needs to understand who her data may be shared with and why

- **What must trustees do?**
  - Ensure that Anita has given express consent to sharing and processing of sensitive personal data
  - Put standard consent provisions in the ill-health application form

- **Any changes?**
  - No

NB Access to Medical reports Act 1988
Cyber security and data protection
Round up – what can trustees do?

- Consider whether existing privacy notices are adequate
- Assess whether service contracts with providers are adequate
- Analyse your cyber-security risk
- Adopt security policy (physical security, on-line security, staff training, etc)
- Take technical advice and keep it updated
- Question administrator / other providers / employer as to their security systems (eg firewalls, access controls); ISO27001 accreditation
- Agree communications protocol and pre-prepared announcements and other steps to minimise impact in case of breach
- Review whether cyber security adequately covered in insurance policies
- Government's Cyber Essentials Scheme
- Others?
"Hogan Lovells" or the “firm” is an international legal practice that includes Hogan Lovells International LLP, Hogan Lovells US LLP and their affiliated businesses.

The word “partner” is used to describe a partner or member of Hogan Lovells International LLP, Hogan Lovells US LLP or any of their affiliated entities or any employee or consultant with equivalent standing. Certain individuals, who are designated as partners, but who are not members of Hogan Lovells International LLP, do not hold qualifications equivalent to members.

For more information about Hogan Lovells, the partners and their qualifications, see www.hoganlovells.com.

Where case studies are included, results achieved do not guarantee similar outcomes for other clients. Attorney advertising. Images of people may feature current or former lawyers and employees at Hogan Lovells or models not connected with the firm.