PSIT Independent Trustees

May 2014

Lost laptops and hefty fines: the perils of data protection

PSIT opinion by:
Kathy Trusler, Scheme Manager

Our existing data protection laws have ensured compliance with EU requirements that have been in place for nearly 20 years now. Saying the world has moved on seems like an understatement. 20 years ago most of us didn't use email; it was the preserve of universities and large multi-national businesses who were beginning to introduce Lotus Notes (remember that?).

The **technological transformation** we have seen in the past two decades has been incredible. This **brings with it new challenges for protecting personal data**, and the EU is playing catch up.

It is all too easy to assume that data is being properly protected. **For pension schemes, the buck stops with the trustees.** Stories in the news of lost or stolen laptops containing unencrypted data should make any trustee nervous. In 2013, Glasgow City Council was fined £150,000 for loss of just 2 of the 74 laptops they discovered were missing.

Existing data protection requirements

Although the EU will be making changes to the data protection directive, the new proposals retain the spirit of the existing framework. So, here's a brief reminder of a trustee's existing responsibilities.

→ Trustees are data controllers and must comply with data protection laws (currently the Data Protection Act (DPA) 1998). This includes **obligations for collecting, using and storing data**.

→ These are underpinned by **eight data protection principles**:

1. Personal data shall be processed fairly and lawfully.
2. Data can only be collected for a specified and lawful purpose, and should not be used in a way contradictory to that purpose.
3. The data collected should be adequate, relevant and not excessive in relation to the original purpose.
4. Personal data should be accurate and, where necessary, kept up to date.
5. Data should not be kept after the initial purpose is complete.
6. All data shall be processed in accordance with all the rights contained in the DPA.
7. You are accountable for the loss or misuse of data, or damage to it, and must ensure appropriate security measures are in place.
8. Data should not be transferred to a country or territory outside the European Economic Area unless it can ensure an adequate level of protection for the rights and freedoms of data subjects.

Continued…

→ Safeguarding data is vitally important. There are some simple steps trustees should be taking, such as:

- using **encryption and secure data transfer** sites
- removing personal data from communications (e.g. National Insurance number) and **replacing with a unique identifier**
- **never emailing unsecured attachments** – sending an unsecured file is risky in itself, but that risk is multiplied when someone 'replies to all' or forwards the email and forgets to remove the attachment.

Including data in the main body of an email and NI numbers in the subject heading are just two examples of bad practice I have been surprised to receive. To avoid slipping into bad habits, **the Information Commissioner's Office (ICO) data sharing checklists** are worth re-visiting regularly.

→ The **biggest risk for trustees is outsourcing** activities to third parties or the sponsoring employer (if the scheme is administered in-house). This risk needs to be minimised by ensuring third parties have systems and safeguards in place to protect and maintain information security and comply with the DPA.

→ Trustees then need to check regularly that these safeguards remain in place – perhaps it is sensible to include the ICO annual renewal on **the scheme's business plan and risk log**, and set up a direct debit for the renewal fee if possible.

→ Trustees also need to ensure **written agreements** in place with providers enable them to **hold the third party accountable if a breach does occur**, for example through the loss or mishandling of data. Recent guidance from the ICO has clarified that professionals who provide specialist services (such as actuaries, accountants and solicitors) are joint data controllers along with the trustees, rather than data processors. This also needs to be reflected in written agreements.

What does the future hold?

The proposed reforms chiefly reflect the significant changes in technology and increasing globalisation, making regulations regarding the sharing of individual personal data consistent across all EU countries. It will also introduce new provisions for outside countries who do business with the EU, which may apply of your third party administrator uses overseas resource.

Personal data will also become the property of the person the data is about. **Individuals will have new rights**, including:

- **the right to be forgotten** – they will be able to request you delete their private information and you must comply, even if it makes managing your pension scheme very difficult
- **data portability** – this is the right to get a digital copy of the information you hold and transfer it to another company.

Other aspects of the proposed reforms that could affect trustees include changes to the requirements for a Data Protection Officer, and how data can be used to predict things about an individual's life. It is easy to see the latter point could potentially affect scheme valuations, for example. However, as the details are still being debated we need to wait for the outcome before we can start preparing for the new world. Hopefully we will know more after the Justice Ministers' meeting in June 2014.

What do you think?

Share your thoughts with us, email **kathy.trusler@psitl.com**