Hogan Lovells

Personal data security for pension scheme trustees

July 2017

Pension briefing

INTRODUCTION

Cybersecurity and protection of personal data are increasingly to the forefront of concerns for pension trustees. The European General Data Protection Regulation (GDPR), applicable in the UK from 2018, will impose additional requirements on trustees and other data controllers.

Security issues arising out of pension trustees' own use of data and confidential information are often overlooked. These issues can be different from those affecting pension managers or other pension professionals. This note focuses on security concerns from the personal perspective of individual trustees (or individual directors of a corporate trustee) and recommends steps trustees can take to protect themselves.

In this note, we use the term "trustee" to refer to an individual trustee or director of a corporate trustee.

WHAT IS SPECIAL ABOUT TRUSTEES?

Many trustees are not pension professionals but, instead, may have other "day jobs" within the sponsoring employer, or be retired from a role within the sponsoring employer's group. Trustees who are professionals are usually not employed by the sponsoring employer, but rather represent third party professional firms which act as trustee for a number of unrelated schemes. This means that, unlike the sponsoring employer's pension manager, human resources director, and other individuals in the employer's HR function, whose day to day roles are concerned with administering benefits, the trustees spend most of their time on activities unrelated to their scheme.

HOW DO TRUSTEES ACCESS SCHEME INFORMATION?

Many trustees will not, in their day job, have access to the sponsoring employer's computer system. Even those employed by the sponsoring employer may have access to a different part of the IT system to that concerning the pension scheme, or they may work in a role which does not involve use of computers. Trustees may routinely carry out trustee duties, such as reading meeting papers, from their home or another location outside the employer's premises (including on public transport), and may do so using laptops or other devices they own personally. In addition, many retired trustees commonly use their personal email addresses for their trustee work.

WHY DOES DATA SECURITY MATTER?

Protection of data matters to trustees as they may face legal liability if data security is breached. Under data protection legislation special provisions apply in relation to members' personal data, and breaches may have to be reported to the Information Commissioner. Leaks of sensitive information about the sponsoring employer may be commercially damaging. A leak of members' confidential information could put them at risk of identity theft or other fraudulent activity.

WHAT INFORMATION DO TRUSTEES USUALLY ACCESS?

A typical trustee will regularly access:

- Reports and advice on the scheme's funding from the scheme actuary;
- Investment reports from the trustees' investment consultant and investment managers;
- Administration reports from the scheme administrator, which may contain member information (including reports of death benefits paid out);
- Legal advice from the trustees' legal adviser;
- Financial information about the scheme's sponsoring employer and, where relevant, any group company which guarantees the sponsoring employer's obligations to the scheme;
- Analysis of the covenant of the employer (and of any guarantor) from a professional covenant adviser;

- Personal details of members about whom decisions must be taken, especially concerning applications for ill health early retirement, or distribution of death benefits.

Information containing member data is likely to be subject to the requirements of data protection legislation including a requirement for the data to be processed securely. Other information listed above is likely to be commercially sensitive.

HOW CAN TRUSTEES PROTECT THEMSELVES?

Trustees should review their own arrangements for accessing sensitive data and should implement tighter security procedures, where appropriate. In practice, asking the sponsoring employer for help from its own in-house IT security team, or from its external IT consultant, may be the most efficient means of doing this. In particular, we recommend that trustees adopt a data security policy which covers their personal use of data. Areas the policy should cover include the following:

- **Email addresses**: use of trustees' personal email addresses for confidential communications increases risk unnecessarily. The employer may be reluctant for trustees who no longer work in its organisation to use an email address similar to that of its employees. However, email addresses in a format such as *name.surname@ABCpensionscheme.co.uk* could be considered.
- **Electronic devices**: requiring trustees to use their own PC, laptop or tablet to access trustee papers increases the risk of security breaches, whether through the device being used by other members of the trustee's family, or through viruses etc being imported when the device is used for other purposes. In addition, the employer's IT support team may be less able to help deal with security breaches through a personal device. Some pension schemes supply their trustees with tablets on which to access trustee papers and email – employers may consider that the additional cost of doing so would easily be outweighed by the increased security this brings.
- **Passwords**: strong passwords should be required when accessing confidential information, including when switching on a device on which scheme information has been downloaded; accessing scheme information from an extranet; or opening attachments to emails. This will be easier to enforce when trustees access scheme information through a device supplied by the scheme or employer.
- **Security of devices**: trustees should agree to take steps to keep their devices physically safe and to lock their screens when moving away from their desks. Requiring use of a screensaver which automatically comes on after a short period of inactivity may be sensible. In addition, trustees should know whom to contact (available 24 hours) if their device is lost or stolen. A device provided by the employer or scheme will be simpler to wipe clean of sensitive data in case of loss or theft.
- **Encryption of attachments**: many schemes are careful to require passwords to access documents stored on scheme extranets, but send confidential documents as attachments to email without use of a password or encryption. A review of trustees' security arrangements should uncover such discrepancies, enabling them to be addressed.
- **Security of hard copy documents**: trustees should review how they handle and store hard copy documents containing confidential information. Storage of documents can be a particular concern for trustees who do not work within the sponsoring employer – it can be good practice for the secretary to the trustees to collect and destroy confidential papers at the end of trustees' meetings.
- **Accessing confidential information / holding confidential conversations in public places**: trustees should be reminded to avoid reading confidential documents or holding confidential conversations (including telephone calls) in public places, such as cafés or trains where they could be overlooked or overheard by others.
- **Use of members' names in trustee papers**: risks of breaches of members' privacy will be reduced if papers containing personal information are anonymised. This will be particularly relevant in relation to death benefit and ill health cases.
- **Disaster recovery**: breaches of data security can occur even when robust security procedures are in place. Trustees should ensure that they know whom to contact in case of a breach and what immediate steps should be taken. Trustees should have round the clock access to emergency support if needed. In practice, this may be provided through the sponsoring employer's own disaster recovery processes.

KEY HOGAN LOVELLS PARTNERS

Katie Banks	**+44 20 7296 2545**	**katie.banks@hoganlovells.com**
Duncan Buchanan	**+44 20 7296 2323**	**duncan.buchanan@hoganlovells.com**
Claire Southern	**+44 20 7296 5316**	**claire.southern@hoganlovells.com**
Edward Brown	**+44 20 7296 5995**	**edward.brown@hoganlovells.com**
Faye Jarvis	**+44 20 7296 5211**	**faye.jarvis@hoganlovells.com**

About Pensions360

Hogan Lovells' broad cross-practice capability covers the full spectrum of legal advice from lawyers who understand pension clients; advising on issues from scheme investments, corporate restructurings and transactions, to funding solutions and interaction with the Regulator or the courts. The ability to draw on specialists from other practices who are not only experts in their field but have an in-depth understanding of pension issues sets us apart from our competitors.

www.hoganlovells.com