PASA Data Working Group

Securing Tomorrow: Essential Steps for Trustees and Pension Providers to Protect Member Data

August 2025

Produced in partnership with:

pwc

Our Experts for Data:

PASA

Acknowledgements

PASA is grateful to the members of the PASA Data Working Group (DataWG) who authored the updated Guidance and their employers:

Chris Tagg (Board Sponsor)	**PASA Board Director**
Kristy Cotton (Chair)	**PwC**
Adam Scarff	**Tesco PLC**
Claire Fuller	**First Actuarial**
Hannah Blomfield	**Intellica**
Julie Beadle	**WTW**
Louise Donohue	**Heywood**
Paul Rickman	**LCP**
Paul Young	**Capita**

Securing Tomorrow: Essential Steps for Trustees and Pension Providers to Protect Member Data

1. Introduction

Trustees and providers responsible for managing schemes are entrusted with safeguarding the financial futures of their members and with their sensitive personal data. In an era where cyber threats and identity fraud are on the rise, ensuring robust data security isn't just a regulatory necessity, it's fundamental to maintaining trust and confidence.

Understanding the threats

Identity fraud and data breaches present a significant challenge for schemes. The detailed personal information held, such as national insurance numbers, dates of birth, addresses, employment histories and financial details, represent a prime target for cybercriminals. If compromised, this data can lead to devastating financial losses for members, and organisations through reputational damage and erosion of trust.

Key Security Risks

Cyber attacks are becoming more sophisticated, seeking out vulnerabilities in systems to steal data. Common security risks include inadequate encryption, weak access controls and failing to stay updated with regulatory requirements such as GDPR. Insider threats from human actions adds another layer of complexity, whether from negligence or malicious intent, and are arguably the biggest weakness in data security. In addition, third-party technology and service providers can introduce additional vulnerabilities if they don't uphold strong security standards.

With the launch of Pensions Dashboards, the potential access to personal data for pension schemes significantly increases, and the data security requirements for trustees, administrators, providers and holders of data are critical.

2. Steps to strengthen data security

Implement data access controls, advanced encryption and multi-factor authentication (MFA)

Role-based access controls should be used with strict user permissions, enforcing least privilege principles. All member data should be protected with up-to-date encryption technologies both in storage and during transmission. Login security can be enhanced by requiring additional verification steps, such as biometric data or one-time codes. This is the first line of defence against unauthorised access. Trustees should review internal controls or assurance reports of their third-party-administrators to review for this security measure.

Secure file transfer platforms should be used where data is shared between service providers, with personal data minimised and sending only the data required for the services to be provided. Technology security

continues to advance, alongside the advancement in the cyber risks, and it's important to monitor processes and continually adopt improvements.

User Training

Most data breaches arise from human action. It's critical to regularly update administration and service provider teams, users and the trustee board on the latest security protocols and phishing threats. Well-informed personnel are crucial to preventing breaches and ensuring a culture of security awareness within the organisation. Data should be included in third party-administrator staff and trustee training plans and logs, with training refreshed annually together with ongoing activities such as phishing testing.

Conduct regular security reviews

Frequent reviews should be scheduled to assess data security and lines of defence and ensure these remain up to date. These include compliance with relevant regulations as they develop, technology enhancements as threats evolve and identification of potential vulnerabilities to be addressed. We may expect trustees to incorporate this within their Effective System of Governance (ESOG) and Own Risk Assessments (ORA) under the Pensions Regulator's (TPR) General Code.

Use secure communication channels

Consideration should be given to how member communications and secure communication channels, such as member portals, should be adopted where possible. Sensitive and personal data is often contained in communications and some methods can have a high risk of data errors and data interception if the accuracy of the communication channel isn't highly maintained. For example, not having accurate and up to date address data for postal communications and the use of unverified personal email addresses for email communication. Data security is an important consideration in developing an effective communication plan. A decision on how data security will be managed within communications should be documented, both for ongoing and project-based requirements.

Develop incident response plans

Administrators and trustees should both prepare detailed response strategies for potential data breaches. Having a clear plan enables swift action, minimising damage and maintaining member trust. These should be

set out in the scheme's **Data Management Plan** and should include steps such as notifying stakeholders and other service providers, seeking advice, and communication and reporting processes.

It's also important to ensure data is stored in secure, compliant environments (e.g. ISO 27001-certified data centres) and regular, encrypted backups are maintained.

Carefully vet and monitor third-party providers

Trustees should ensure any third-party providers comply with stringent security standards. Their security weaknesses can become the scheme's liabilities, so thorough vetting and regular monitoring is essential. Trustees should set out how they will vet and monitor providers, including the frequency and approach to be taken, seeking independent support where appropriate.

Data will be held by providers other than administrators, e.g. actuaries, communication providers, data specialists and auditors. It's important all providers comply with strict data security procedures.

Consideration should be given to seeking specialist cyber security services to support the development and ongoing monitoring of policies, processes and suppliers.

Be careful with AI

AI uses data, and where data is shared with AI, it's typically stored within the AI going forwards. It's important to understand the implications of using AI on the access and storage (including location) and uses of a scheme's data.

The PASA Data Working Group will shortly be issuing Guidance on the responsible use of AI in pensions administration.

3. TPR's Guidance

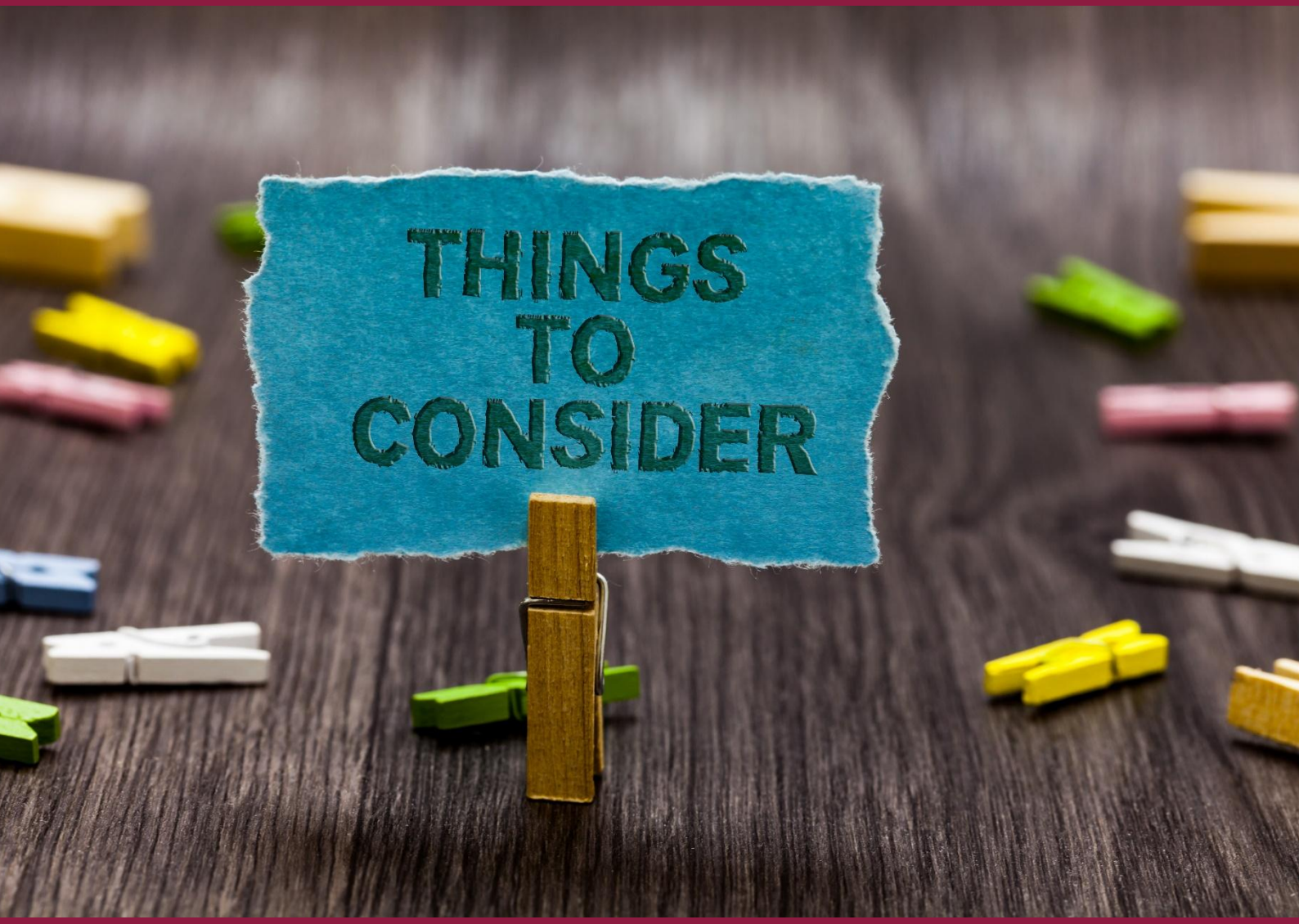
The Pensions Regulator has issued **Cyber Security Guidance for pension schemes** and is encouraging the largest and highest risk schemes, their advisers and suppliers to fully meet the expectations set out in the **National Cyber Security Centre** (NCSC) **10 Steps to Cyber Security Guidance**. Smaller schemes and lower risk suppliers should consider the controls as set out in the NCSC's **Small Business Guide: Cyber Security.**

4. Peace of mind in data security

In the face of ever-evolving cyber threats, it's imperative for trustees and providers to take a proactive and dynamic approach to data security. While technology plays a crucial role, fostering a culture of transparency and continuously engaging in training and collaboration with industry counterparts can significantly bolster the scheme's defences.

By prioritising data security, members' trust is reinforced their scheme, ensuring they can look forward to their retirement with confidence. Protecting sensitive member data isn't just about mitigating risks; it's about safeguarding the integrity of the scheme and the peace of mind for all involved.

PASA



Get in touch:

info@pasa-uk.com

www.pasa-uk.com

PASA is a Community Interest Company and our full name is Pensions Administration Standards Association CIC. Company number: 6597097