Data governance

November 2025

Sackers

With changes to data protection legislation and staging dates for connection to pensions dashboards underway, now is a good time for trustees to take stock of their data governance.

Data protection changes

The Data (Use and Access) Act 2025 (the "Act") received Royal Assent on 19 June 2025 and is coming into force in stages. Whilst the Act is not making wholesale changes, it will impact the way in which schemes operate in some areas, with action needed as a result.

Data subject access requests ("DSAR")

- When dealing with a DSAR, trustees as data controllers are now only required to undertake "reasonable and proportionate" searches for relevant information.
- The one-month time limit for responding to a DSAR will start from the latest of the trustees receiving:
  - the request
  - any information requested to confirm the data subject's identity, or
  - payment of a fee, if this has been requested for responding to a "manifestly unfounded" or "excessive" request.
- Trustees will be able to "stop the clock" to ask for clarification of a DSAR (provided they can demonstrate it is reasonable for them to do so). If clarification is requested, the time limit is paused until it is received. It will also be possible to extend the time limit, by two further months, by notice to the data subject where this is necessary due to the complexity and/or number of requests.

These changes broadly codify current ICO guidance.

Action

Trustees should ensure their DSAR processes are revised, where necessary, to address the above.

Complaints

Data protection complaints can come from anyone who is unhappy with how the trustees have handled their personal information. For example, they might be dissatisfied with a response to their DSAR or have been impacted by a data breach.

Specifically, the Act will require trustees to:

- give members a way of making complaints to them – this could include providing a complaint form that people can submit either electronically or in writing. The ICO expects data controllers (including trustees) to put a written complaints procedure in place and to publish it on their website
- acknowledge receipt of complaints within 30 days of receiving them
- take appropriate steps to respond to complaints, including making enquiries, without undue delay and keeping people informed about progress
- tell people the outcome of their complaints without undue delay.

The ICO has consulted on draft complaints guidance which explains what organisations must, should and could do to comply with the new requirements.

Action

Trustees should devise and record a process for handling data protection complaints and update the information in their privacy notice on the right to complain. Given the difference in timescales, it will be important for members to understand that this complaints process does not form part of the scheme's IDRP and for trustees to ensure their complaints team can recognise the different types of complaint. It will be worth considering how to manage the two separate sets of requirements and the extent to which alignment is helpful.

The Act's complaints provisions are expected to come into force in June 2026.

Sackers

Other areas of interest

Cybersecurity

Always important for trustees, cyber security is back in the headlines with the ICO's announcement that Capita is being fined £14m for its 2023 data breach. John Edwards, UK Information Commissioner, called on "every organisation, no matter how large, [to] take proactive steps to keep people's data secure", warning that cyber criminals "don't wait, so businesses can't afford to wait either – taking action today could prevent the worst from happening tomorrow."

Action

All trustees should regularly assess both their and their service providers' cyber security, making changes where appropriate (see our Hot Topic, "Cyber security – is your scheme prepared?"). In the worst-case scenario of a cyber breach impacting a scheme or its members financially, trustees should liaise with their legal advisers to understand their position and the extent to which it may be possible to recoup any losses.

Monitoring and managing the use of AI

Chances are that if your service providers aren't already using AI in their systems, they soon will be.

Action

To ensure risks are mitigated and members are appropriately protected, trustees should:

- investigate and evaluate the service provider's proposals – How does their AI tool work? What personal data is being processed? What other information does the AI tool utilise? What security measures are in place? What is the AI tool designed to do? Once you understand the position, consider whether this raises any points that should be addressed by setting parameters in your service agreement
- consider introducing an AI policy and providing training – trustees should understand AI and a policy is a useful way to record key principles such as expectations for AI use and data protection considerations. Training will need to be revisited at suitable junctures so that trustees stay on top of developments.

Data, dashboards and DPIAs

A data protection impact assessment ("DPIA") is a process designed to help organisations to systematically analyse, identify and minimise the data protection risks of a project or plan.

Views differ on whether a DPIA is essential in relation to dashboards, with TPR's guidance leaving it as a question for trustees. However, the ICO makes clear that "combining, comparing or matching personal data obtained from multiple sources" is a "high risk activity" which requires a DPIA. The PDP likewise indicates that they are expected and must reflect the large-scale processing that will be undertaken.

Action

A DPIA can be undertaken wherever you are in your dashboards journey. Liaise with your usual Sackers contact about what steps to take.

Sacker & Partners LLP
20 Gresham Street
London EC2V 7JE
T +44 20 7329 6699
E enquiries@sackers.com
www.sackers.com

If you have any questions on any of the above, or would like further information, please speak to your usual Sackers contact.