Getting ready for GDPR

Maggie Williams reveals how pension schemes are to prepare for the General Data Protection Regulation (GDPR), which comes into force on 25 May 2018

While some aspects of GDPR are an evolution of current Data Protection Act practices, and others simply reflect good scheme governance, there is still plenty that trustees need to do to make sure their schemes are compliant.

Know your scheme data – and who uses it

The first step towards GDPR compliance is for schemes to understand their data, and who has access to it. Key questions are:

- what personal data they hold
- who they hold it in relation to
- how long they have held it for
- who they share it with, and
- if any of that information is used outside the UK.

GDPR defines two roles within data management: the data controller (who is responsible for ensuring compliance with GDPR) and data processors (who handle data and, under GDPR, also have statutory obligations). In many businesses, both the data controller and data processors might be employees within the same company – but for pension schemes, the situation is often quite different. The trustees will be a data controller, but most data processors will be third parties, others, including the sponsoring employer in this context. Some of those third parties will also be data controllers in their own right.

Trustees need to identify all of their data processors, and how data flows between them. While some of these will be obvious – such as the sponsor and scheme administrator – there are others to consider as well. "More of a challenge is to identify less obvious data flows and data processors," says Willis Towers Watson associate director Helen Nicholas. "What about the printers who print and distribute member newsletters? What about the doctor who assesses ill-health retirement cases?"

What to do now? Carry out a data mapping, or data audit, exercise to identify the types of data that the scheme (and its third parties) hold, who its data processors are, and how they interact.

Update contractual arrangements

Once trustees know who their data processors are, they will need to update any contract arrangements to reflect GDPR rules. This is particularly important if a third party is also a data controller in their own right (such as the scheme sponsor). "Another data controller will have their own obligations under GDPR, so the contract should specify exactly what the other party can use scheme information for," says Sackers partner Claire Carey.

In some instances, data will be managed by joint controllers who need to work together to decide how it will be used. "This is particularly important when it comes to individuals' rights," says Carey. "You will need to decide together who is responsible for responding, should an individual want to know what information is held about them."

What to do now: Contractual updates are one of the most important and time-consuming aspects of GDPR preparation. But, most of the work is a one-off exercise. Reviewing contracts over time should then be less onerous.

Update privacy notices

Although most schemes will already have a privacy notice, the information that needs to be included under GDPR is wide-ranging and must be broad enough to cover all the ways in which a scheme might want to use an individual's data. These include the legal basis for processing information, explaining an individual's right to access his or her data and to withdraw consent for its use, the source of any third-party data, and the right to rectify or erase data held about an individual.

This all needs to be included in a single notice, which is available to scheme members and potential members.

What to do now: Make sure that all members have access to the full privacy notice. "There is an option to signpost the full privacy notice from a shorter format document," explains Carey. If the scheme usually sends out printed information to scheme members, the full privacy notice must also be available as a printed document.

Understand individuals' rights

Any member can ask about the information the scheme holds about them and ask to see it (termed a subject access request). They can also ask for out-of-date information to be corrected without undue delay or deleted altogether.

Once GDPR becomes law, members will also be able to object to data processing. "Make sure you have genuine legal grounds for processing information," cautions Carey. Grounds could include the legal requirement to comply with the terms of the trust, pensions legislation, or a legitimate interest on the part of the trustees to make sure the scheme is run properly. Trustees will need to make it clear exactly what their 'legitimate interests' are, however: "Paying the right benefits to the right people is a pretty compelling legitimate reason for holding data," adds Carey.

What to do now: Trustees will need to think about how they apply individuals' rights, and how they and third parties respond promptly to requests for information.

Be breach-ready

Trustees will need to make sure that they (and the third parties they work with) have a clear, documented plan of action, in the event of a data breach. It will also need to document how the scheme protects personal data in the first instance - for example, policies for using data on laptops, or storing information online 'in the cloud'. "Pension schemes hold a goldmine of personal and financial data," says RSM head of pensions Ian Bell. "Trustees need to take their obligations seriously, particularly under GDPR." There are significant fines for not doing so - failure to notify authorities of a data breach carries a fine of up to €10 million or 2 per cent of annual turnover, in addition to the €20 million or 4 per cent of annual turnover fine for breaching the regulations.

What to do now: Schemes will need to make sure they have a clear policy in place that explains what happens if there is a data breach, and how this will be reported within the required 72 hours turnaround time.

Written by Maggie Williams, a freelance journalist

Case study: The MNOPF

With over 25,000 members and 80 years of history behind it, the Merchant Navy Officer's Pension Fund (MNOPF) had its work cut out when it came to preparing for GDPR. MNOPF pensions director Ivan Laws explains how the scheme approached it.

What have been the major challenges involved in preparing for GDPR, and how have you addressed them?

The principle issue we faced (and are facing), was initial industry-wide inertia. Only when headlines about the magnitude of potential fines began to surface, did panic set in across pensions as a whole.

The Information Commissioner's Office (ICO) has provided a level of reassurance (without being too specific) by stating that it will take a pragmatic approach to GDPR implementation on and after 25 May.

However, the ICO has not given any industry-specific advice to pension schemes. Even at this stage there is uncertainty about how certain areas of the GDPR will be applied in a pensions context. This may be because pension schemes are not the primary target of the regulations, but sadly that is not a view our industry can sensibly take!

Is there anything that you would do differently if you were starting the process again?

If you think about the hundreds of pension schemes that are individually consulting their legal advisers and the attendant costs, it would be good to think that the pensions industry could adopt a more collective approach to regulations such as GDPR. That way, general principles (such as grounds for processing being a legitimate interest) could be established quickly and cost effectively, with individual scheme advice then being required on a much smaller scale, at much less cost.

What guidance would you give to a scheme that is still working on its approach to GDPR at this stage?

I suspect that the majority of schemes will still be working on GDPR. The advice I would give is to do what we have done, and that is to put together a comprehensive list of tasks in the form of a plan to fully implement the provisions of GDPR. This will go beyond 25 May. Give emphasis to the tasks that carry the greatest risk. They will be those directly related to members, such as data processing permissions and data retention policies. It's time to find out what is in all those old boxes!