HOW WELL DO YOU KNOW YOUR DATA?

GETTING READY FOR THE GDPR

PART TWO

UNDERSTANDING YOUR SCHEME'S DATA

GOWLING WLG

UNDERSTANDING YOUR SCHEME'S DATA

Data controllers are responsible for the processing of personal data. In order to comply with their legal duties, data controllers need to understand what personal data they hold, what they do with it and who they share it with.

KEY POINTS

Trustees need to understand their scheme's data

Data controllers will only be able to comply with legal duties under the GDPR if they have a good understanding of the personal data that they control. Data mapping is simply assessing who processes what personal data and why they need to do so.

Trustees can only use third parties providing 'sufficient guarantees'

Under the GDPR, data controllers can only use third party data processors that provide 'sufficient guarantees' that they will implement 'appropriate technical and organisational measures' to ensure compliance with the GDPR. Data mapping is often the first stage for trustees in assessing their third party service providers.

Questionnaires can help with data mapping

A questionnaire or checklist can help to produce a systematic and standardised data mapping exercise. Trustees should ask themselves and third parties a range of 'who, what, where, why, when and how' as part of a data mapping exercise.

Decide who is responsible for doing what and set a firm deadline

Understanding your scheme's data is an essential first stage in a data protection compliance project. The responses to the questionnaire will help the trustees and their advisers with the other essential compliance work. It should, therefore, be project managed with a firm deadline for completion.

Why is it so important for trustees to understand a pension scheme's data?

In order to comply with their legal duties under the GDPR, data controllers need to understand the personal data that they process. For example, data controllers are required to provide certain information to data subjects (also known as a privacy or fair use notice). As part of this information, data controllers have to set out:

- the categories of personal data that are processed;
- the categories of data subjects to whom this personal data relates;
- the data controller's legal grounds for processing the personal data; and
- anyone who the data controller shares the personal data with.

Trustees will need to understand their scheme's data before they can pass on this information to members.

Do your third party service providers and professional advisers provide sufficient guarantees?

In addition, data controllers can only use data processers that provide sufficient guarantees that they will take appropriate technical and organisational measures to comply with the GDPR. Understanding the scheme's data and the role played by third parties in processing the scheme's data will be the first step for many trustees in assessing whether their third parties provide sufficient guarantees.

Why is this process particularly relevant for many pension scheme trustees?

Many trustees are unusual as data controllers as they do not process the personal data that they control on a day to day basis. Instead, many trustees rely on third parties to administer their scheme. These third parties can be third party providers of pension scheme administration services or administration services provided by one of the scheme's employers.

In addition, trustees rely on third parties for professional advice. Actuaries, lawyers and investment consultants may receive personal data from the trustees so that they can provide this advice.

Finally, because of the nature of pensions, trustees may need to use other, more specialised third parties from time to time. Trustees will need to provide personal data to some of these third parties (e.g. tracing services, independent medical advisers and online document and meeting management providers) for them to be able to carry out work for the trustee.

How can trustees get a clearer understanding of their scheme's personal data?

The process of getting a clearer understanding of scheme data is being referred to by many in the pensions industry as data mapping. Although this sounds like a technical process, it is, in reality, just a methodical audit of the scheme's personal data. Depending on the circumstances, this process can be led by the trustees, the scheme's administrators, the scheme's lawyers or another third party.

In order to approach data mapping in a systematic way, many trustees are using a questionnaire or checklist and also asking the scheme's third party service providers and professional advisers to consider and fill out the same questionnaire or checklist. There are no set questions for questionnaires, but they can all be summarised as asking variations on standard questions:

- **Who**
  - who does the scheme's personal data relate to? Who are the data subjects?
  - who do the trustees share the scheme's personal data with?
- **What**
  - what categories of personal data are processed? For pension schemes, this will include members' names, addresses, national insurance numbers and bank details.
  - what types of special category (i.e. sensitive) personal data are processed? For pension schemes, this will include members' health records obtained as part of applications for ill-health early retirement.
  - what role do third parties have in relation to the scheme's data? Are they data processors? Are they joint data controllers with the trustees? Or are they processing data as standalone data controllers?
- **Where**
  - where is the scheme's personal data processed? The main consideration here is whether personal data is processed in a country that is not a member state of the European Union. The GDPR requires additional safeguards when personal data is transferred outside of the EU.
- **Why**
  - why is the personal data processed? This is intended to provide details for determining the trustees' legitimate interests in processing the personal data (or having the personal data processed by a third party on the trustees' behalf).

- **When** – when, and for how long, is the personal data processed. This is intended to help the trustees consider storage limitation and retention periods.
- **How** – how is the scheme's personal data processed? What security measures are applied to the processing and transfer of paper and electronic records?

What are the main things that pension scheme trustees will have to think about?

Understanding the scheme's data is an essential part of getting ready to comply with the GDPR. It will be difficult, if not impossible, for trustees to comply with other legal requirements if they do not know what personal data they process, why they process it and who they share it with. Trustees should think about the following key issues:

Who will carry out the data mapping exercise?

Trustees are usually data controllers and they are ultimately responsible for the scheme's data. Many trustees do not, however, deal with their scheme's data on a day to day basis. Trustees may, therefore, ask a third party (such as the scheme's administrator or legal advisers) to carry out the data mapping exercise. Whoever carries out the exercise, trustees should make sure that it is clear who is responsible for doing what and set a firm deadline.

What questions will you ask yourselves and third parties?

The results of your data mapping exercise will only be as good as the questions that you ask. You might find it useful to think about your legal duties under the GDPR and design your questionnaire so that the responses will help you comply with these legal duties.

Who will review the completed questionnaires / checklists?

What will happen once you and your third parties have filled in questionnaires? How will you incorporate a third party's standard response into your review? Ultimately, the information gathered in a data mapping exercise will be used to help the trustee comply with specific legal duties under the GDPR. A standardised report based on the scheme's questionnaire will make it easier to take the required next steps.

How will you assess whether third parties provide sufficient guarantees?

Trustees will need to consider a range of evidence to determine whether their third party service providers and professional advisers provide sufficient guarantees as required under the GDPR. Some of this evidence will come from responses to the trustees' data mapping exercise. Trustees may want to put together a pack containing evidence for each of the relevant third parties.