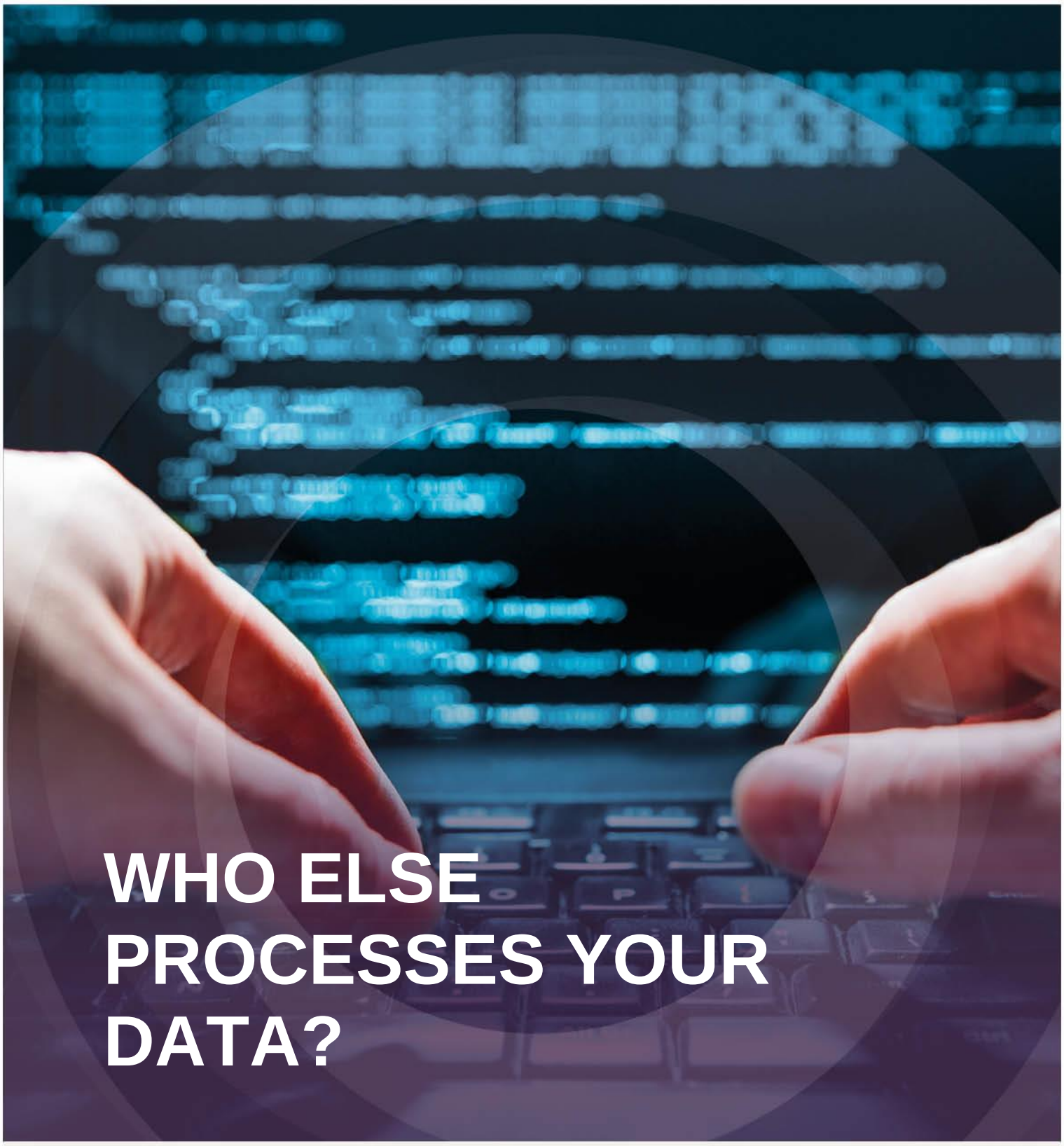

WHO ELSE PROCESSES YOUR DATA?

GETTING READY FOR THE GDPR

PART THREE

DEALING WITH THIRD PARTIES

GOWLING WLG

DEALING WITH THIRD PARTIES

Under the GDPR, data processors will, for the first time, have direct legal duties under data protection legislation. Many pension scheme trustees use third parties for professional advice and to help run their schemes. What will trustees have to do to ensure compliance by these third parties?

KEY POINTS

Trustees usually rely on third parties

Third parties usually play an important role in the running of a pension scheme. Service providers and professional advisers need to use the scheme's personal data in order to help trustees run their scheme.

Certain contractual terms need to be in place between trustees and third parties

The GDPR requires specific terms to be in place between data controllers and data processors. These include general statements and stipulations that data processors must be able to give.

Third party data processors must provide sufficient guarantees

Under the GDPR, data controllers can only use third party data processors that provide sufficient guarantees that they will comply with the GDPR. Trustees will need to carry out due diligence on their third party service providers and professional advisers to determine whether they provide sufficient guarantees.

Trustees will need to gather and retain evidence of how third parties comply

Contractual terms are not enough – third parties will need to provide evidence of how they comply. This might come in the form of a standard form statement explaining the data and security measures that the third party has put in place. Trustees should keep records of this evidence to demonstrate their own due diligence.

Why are third parties particularly relevant for pension scheme trustees?

Many trustees rely on third party service providers to administer their pension schemes. For such schemes, the bulk of data processing is carried out by third parties. In addition, trustees have to appoint professional advisers such as actuaries and lawyers. These advisers usually have to use the scheme's personal data in order to provide advice.

What third parties do trustees need to think about?

Pension scheme trustees need to think about any third parties that process the scheme's personal data on behalf of the trustees. For most pension schemes, this will include:

- scheme administrators (including employers that provide scheme administration services);
- professional advisers (including the scheme's actuary and legal adviser); and
- other third party service providers (including beneficiary and missing member tracing services, independent medical advisers, online document and meeting platform providers and any other third party service provider that processes the scheme's personal data on behalf of the trustees).

What legal duties will trustees have in respect of third parties?

There are two main legal duties that apply in respect of third parties:

1. Are the required contractual terms in place?

Pension scheme trustees are data controllers for the purposes of the scheme's personal data. Under the GDPR, data controllers have to ensure that there is a legally binding contract in place between them and any third parties that process the scheme's personal data on behalf of the trustees. The GDPR specifies a range of terms that need to be included in a contract between data controllers and third party data processors.

2. Does the third party provide sufficient guarantees?

Under the GDPR, data controllers should only use third party data processors that provide sufficient guarantees that they will implement appropriate technical and organisational measures in order to comply with the GDPR and protect personal data. Data controllers will, therefore, need to satisfy themselves that existing third parties provide sufficient guarantees. In addition, when appointing a new third party, data controllers will need to carry out due diligence to ensure that the third party will provide sufficient guarantees.

What are the required contractual terms?

The GDPR requires certain terms to be in legally binding contracts between:

- data controllers and data processors; and
- data controllers and other data controllers when they are joint controllers.

There are three types of terms that may need to be included. If the third party is only a data processor, only the first two sets of terms need to be included. If the third party is a joint controller, all three sets of terms need to be included.

Statements about the processing

In order to be compliant with the GDPR, the contract between a data controller and the data processor should include statements that cover:

- the subject-matter of the processing;
- the duration of the processing;
- the nature and purpose of the processing;
- the type of personal data that is being processed;
- the data subjects or the categories of data subjects whose data is being processed; and
- the obligations and rights of the data controller.

Stipulations that apply to the data processor

In order to be compliant with the GDPR, the contract between a data controller and the data processor should also contain stipulations that the data processor will:

- only process on the documented instructions of the data controller;
- ensure that authorised persons who process the personal data are bound by confidentiality obligations;
- take steps that comply with the GDPR's requirements covering the security of processing;
- only engage sub-processors on the written instructions of the data controller;
- assist the data controller in complying with various obligations such as data subject rights requests and breach notification;
- delete or return the personal data at the end of the contract; and
- be able to demonstrate how it has complied with its obligations under the GDPR.

Provisions covering the relationship between joint controllers

In order to be compliant with the GDPR, the contract between a data controller and another data controller in a joint controller relationship should set out:

- their respective responsibilities, roles and relationship;
- how the parties will comply with the GDPR, in particular dealing with:
- data subject rights requests; and
- communicating with data subjects (i.e. privacy notices)

In addition, the joint controllers need to make the essence of the agreement available to data subjects. This will usually be done via the privacy notice.

How can a trustee assess whether a third party provides sufficient guarantees?

As data controllers, pension scheme trustees should only appoint third party data processors that can provide sufficient guarantees to implement appropriate technical and organisational measures in order to:

- comply with the GDPR; and

- ensure the protection of the rights of data subjects.

Does a contractual term stating that the data processor will implement appropriate technical and organisational measures provide sufficient guarantees?

On its own, no. This is especially the case if the data processors day to day practice does not meet the standards that they have set out in their contract.

It can, however, be part of the evidence that the Trustees will need to satisfy themselves that the third party has provided sufficient guarantees.

Is an external consultancy required?

How can Trustees make a judgment of whether a third party provides sufficient guarantees? Will they need to appoint a consultancy to provide expert advice on data protection and data and cyber security?

This will depend on the situation. It might be appropriate where the Trustees have particular concerns about the data processor. It might also be a good idea if there is a particularly high volume of sensitive personal data.

Trustees that use recognised names in the pensions industry may not need to go this far.

Are there industry standards or codes of practice?

It would make the Trustees life a lot simpler if there was a single standard or code of practice that was independently verified and demonstrated compliance.

There are a raft of British and International standards covering relevant areas of document management and data and cyber security.

Up to this point, however, a single standard or code of practice has not yet emerged.

So, how will Trustees decide?

Trustees are likely to have to weigh up a range of factors. This will include the information that has been provided by the third party – most pensions industry data processors are setting out revised terms and conditions and issuing statements on how they, as an organisation, deal with data protection.

What evidence should Trustees compile?

Evidence that a third party provides sufficient guarantees could come from a variety of sources, including:

- contractual terms (including key performance indicators);
- replies to questionnaires / data mapping exercises;
- replies to specific inquiries;
- statements on how the organisation is planning to comply with the GDPR; and
- data protection and data and cyber security statements.

What are the main things that pension scheme trustees will have to do next?

Make a list of the third parties that process the scheme's personal data

Trustees should consider all of their third party service providers and professional advisers and any other third parties (e.g. the scheme's employer(s)). It might be useful to create a diagram / map rather than a list.

Ask relevant third parties to complete a data mapping questionnaire

Third parties are only relevant for data protection purposes if they **process** the scheme's **personal data**. Processing covers a wide range of activities, but there are exceptions (e.g. Royal Mail is not processing data if they only hold a document or a USB memory key in order to deliver it). If the third party only receives anonymous data or scheme level data that does not identify a living, natural

person, they will not be dealing with personal data and can be discounted from this process.

Ask relevant third parties whether their terms are GDPR-compliant

Third parties are putting in place variations to their standard terms and conditions to deal with the requirements for specific terms under the GDPR. Have all of your third parties provided such variations? Have you had them reviewed by the scheme's lawyers?

Ask third parties how they provide sufficient guarantees

Trustees should ask third parties to provide evidence of how they will comply with their duties under the GDPR. This may come in the form of responses to a questionnaire, a standard form response covering data protection and data and cyber security, a page or section of a website or a combination of these. It is important for the trustees to keep a record of this evidence so that they will be able to demonstrate the due diligence they carried out on their third party service providers and professional advisers.