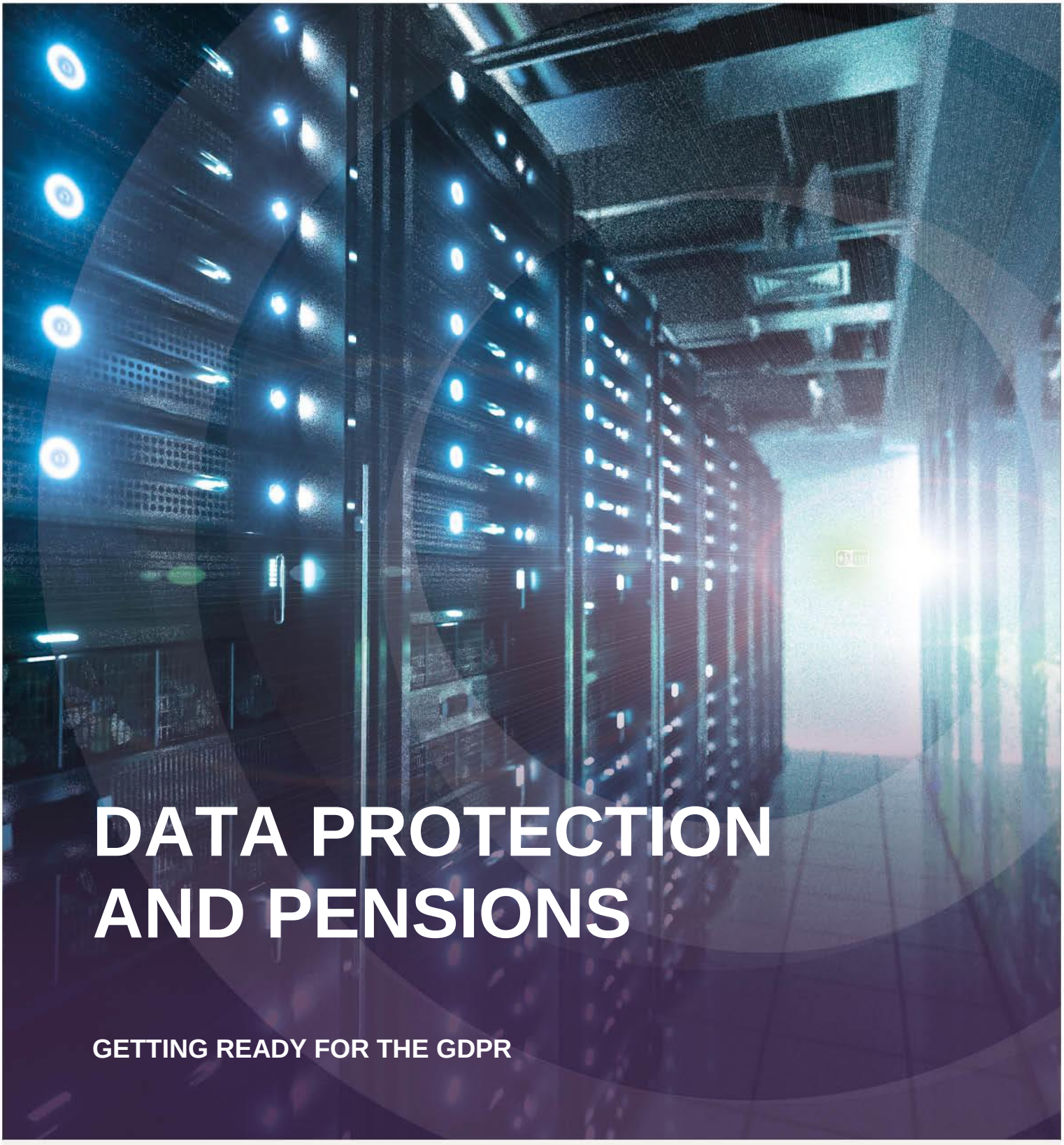


DATA PROTECTION AND PENSIONS

GETTING READY FOR THE GDPR

JANUARY 2018

GOWLING WLG

CONTENTS

ARE YOU READY FOR THE NEW DATA PROTECTION LAWS?

GETTING READY FOR THE GDPR

PART ONE

DATA PROTECTION LAWS ARE CHANGING

GOWLING WLG

DATA PROTECTION LAWS ARE CHANGING

On 25 May 2018, the General Data Protection Regulation (GDPR) goes into effect in all member states of the European Union, including the United Kingdom.

KEY POINTS

The GDPR comes into effect in May 2018

New data protection laws and regulations will come into effect across the EU on 25 May 2018.

The GDPR will apply to trustees

Pension scheme trustees are typically data controllers in respect of a scheme's personal data.

New legal duties and higher fines

The GDPR applies a range of legal duties on both data controllers and data processors. In addition, the maximum levels of fines for data breaches are materially higher.

Trustees will have to take action

As data controllers, Trustees will need to take action to ensure that they comply with the GDPR. This will include making important decisions relating to data protection.

What is the new data protection law?

The new data protection law is the General Data Protection Regulation (the **GDPR**). As an EU regulation, it will apply directly in all of the EU's member states. The GDPR will replace the current data protection regime under the EU's Data Protection Directive 1995 (brought into effect in the UK by the Data Protection Act 1998).

When will the law on data protection change?

The GDPR goes into effect in all EU member states (including the UK) on 25 May 2018. The UK will also have new domestic legislation in a new Data Protection Act. The Data Protection Bill 2017 – 19 is currently passing through Parliament.

What are the biggest headline changes under the new data protection regime?

There are two key changes that will transform how people think about data protection:

1 Data processors will, for the first time, have direct legal duties under data protection legislation

Under the Data Protection Act 1998, only data controllers owed direct legal duties. Under the GDPR, data processors will also have direct legal duties.

In a pensions context, this means that service providers (such as administrators) and professional advisers (such as investment consultants) are likely to press for more comprehensive coverage of data protection issues in contracts and push for stricter delineation of roles, responsibilities and liabilities in these agreements.

2 Fines will be materially higher

Under the Data Protection Act 1998, the maximum fine for a serious breach of data protection law is £500,000. Under the GDPR, the maximum fine will, depending on the type of breach, be either:

- the higher of €20 million Euros and 4% of global turnover; or
- the higher of €10 million Euros and 2% of global turnover.

Most of the obligations under the GDPR fall under one of these two sets of fines.

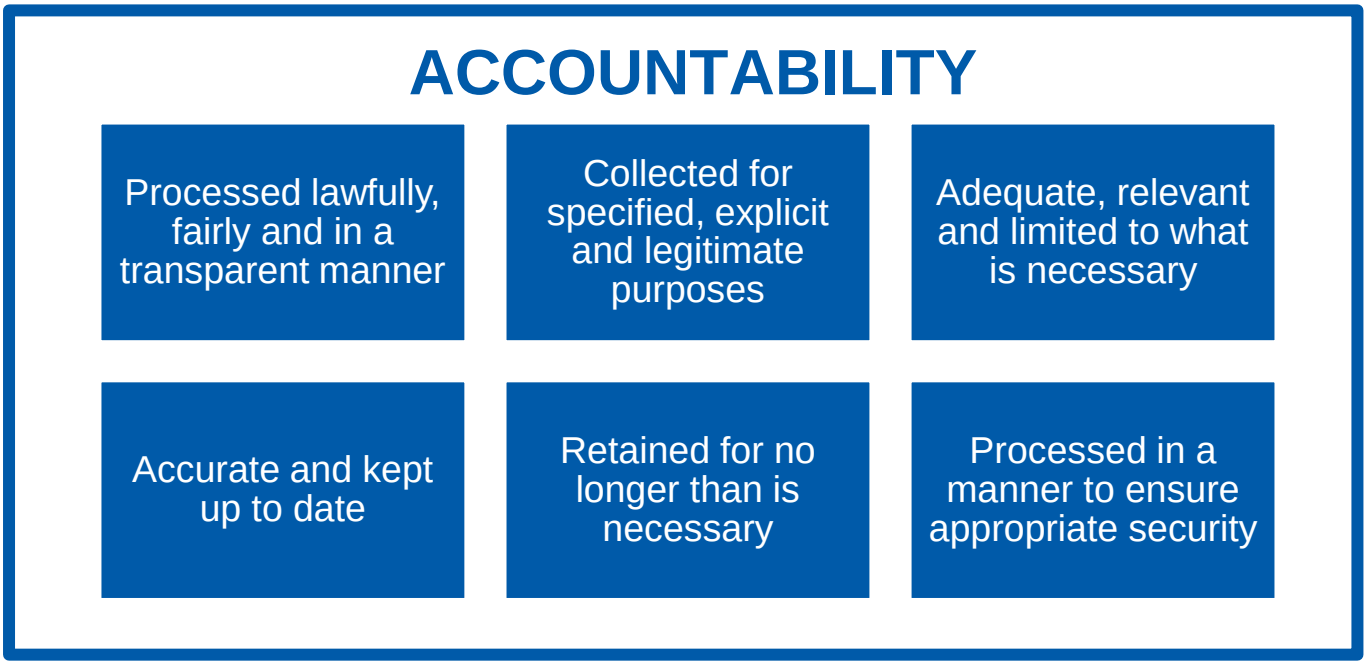
In the pensions industry, this means that data protection issues will be more central to negotiations on contracts and are likely to feature more prominently on everyone's list of priorities. In addition, it is likely that employers will be more concerned to ensure that trustees are complying with their data protection obligations.

What are the data protection principles under the GDPR?

The Data Protection Act 1998 set out eight data protection principles that guided the legislation and regulatory regime. This approach has been followed in the GDPR. There are six principles set out in the GDPR along with an additional overriding principle of accountability that applies to all aspects of the regime:

1. lawfulness, fairness and transparency;
2. purpose limitation;
3. data minimisation;
4. accuracy;
5. storage limitation; and
6. integrity and confidentiality.

In plain English, the principles can be understood as requiring that when personal data is processed, it is:



Why is there also a Data Protection Bill in the UK?

The government has brought a new Data Protection Bill before Parliament. This is not intended to duplicate or transpose the provisions of the GDPR into UK law. Instead, the Data Protection Bill 2017 – 19 will:

1 Extend the scope of the GDPR

The GDPR sets out a general framework, but requires Member State or further EU legislation to provide a comprehensive data protection framework. The Data Protection Bill will provide the UK's 'member state' legislation to ensure that the GDPR works in the UK.

2 Fill in some of the gaps in the GDPR with UK legislation

The GDPR sets out the guiding principles and the general framework for an EU-wide data protection regime. More detailed provisions are then expected to be set out in additional EU or member state legislation. The Data Protection Bill will provide this additional legislation in the UK and will help to ensure that the GDPR works as intended.

3 Set higher standards in respect of control over personal data

The Conservative Party included commitments on data protection in their manifesto in the run up to the General Election held in June 2017. The government is therefore committed to give people more control over use of their data, and providing new rights to move or delete personal data. These will go over and above what is required in the GDPR.

4 Preserve, where possible, the tailored exemptions under the current data protection regime

The Data Protection Act 1998 contains a series of exemptions which help UK businesses, researchers, financial services, journalists and lawyers to do business. The Data Protection Bill seeks, as far as possible, to retain these exemptions and provide continuity for anyone engaged in these areas in the UK.

5 Repeal the Data Protection Act 1998

The Data Protection Bill includes provisions to repeal the Data Protection Act 1998 and to clarify the role of the Information Commissioner's Office. It will also ensure that any provisions of the Data Protection Act 1998 that need to be carried forward are preserved in primary legislation.

The Data Protection Bill **will not** transpose the GDPR into UK legislation. This will be achieved via the European Union (Withdrawal) Bill. The government and the ICO have, however, confirmed that the UK's data protection regime will not be materially changed as a result of the UK's withdrawal from the European Union.

Why is data protection relevant to pension scheme trustees?

The GDPR's main focus is to regulate the processing of personal data. Pension scheme trustees need to process personal data for a number of reasons, including:

- administer the scheme in line with the scheme's governing documents;
- pay the correct pension benefits to the right people at the right time; and
- to exercise discretions and make decisions in line with the scheme's governing documents and their duties under trust law.

Trustees will usually be data controllers in respect of their scheme's personal data. Under the GDPR, data controllers are required to process personal data in line with the data protection principles and comply with a range of specific legal requirements.

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

The GDPR encourages data controllers to put in place:

- data protection by design; and
- data protection by default.

In practice, this means that data controllers (such as trustees) will need to think about the policies, processes and procedures and ensure that they reflect the data protection principles. Trustees should consider the following key issues:

Understand your scheme's data and your legal obligations

Pension scheme data is usually held on paper files and/or computer systems. This data is often shared with third party service providers. As data controllers, trustees will need to understand what personal and sensitive personal data the scheme and any third parties hold, use and share. As a data controller, trustees will be expected to understand their legal duties and demonstrate how they've complied. Part two of this Guide focuses on this in more detail.

Consider the role of third parties and contractual terms

Third party service providers are key to the administration and running of many pension schemes. Trustees need to understand and review how the scheme's administrators, actuaries, lawyers and other advisers use the scheme's data. They will also need to review and possibly renegotiate the contractual terms that are in place with any third parties. Part three of this Guide focuses on third parties in more detail.

Make decisions about legal issues on data protection

Data controllers will need to make decisions on a range of issues relating to data protection. One of the most important decisions will be to agree the legal basis upon which the Trustees process the scheme's personal and sensitive personal data. Trustees will also have to record these decisions in order to demonstrate accountability. Part four of this Guide looks at privacy notices in more detail.

Communicate with data subjects by issuing data protection notices

Data controllers are required to give certain information to individuals about how and why their personal data is used. This is usually done by issuing data protection notices (also referred to as privacy notices). Under the GDPR, data protection notices need to be more detailed and specific than under the current data protection legislation. Part five of this Guide looks at this in more detail.

Review the scheme's policies and procedures

Data controllers need to ensure that they have put in place 'appropriate technical and organisational measures'. This means understanding and reviewing how the scheme (and any third parties) store, secure, share, back-up and monitor personal data. Data controllers will also have to demonstrate how they have complied. A compliance record can help with focusing on the key tasks, managing the compliance project and documenting the steps taken.

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?

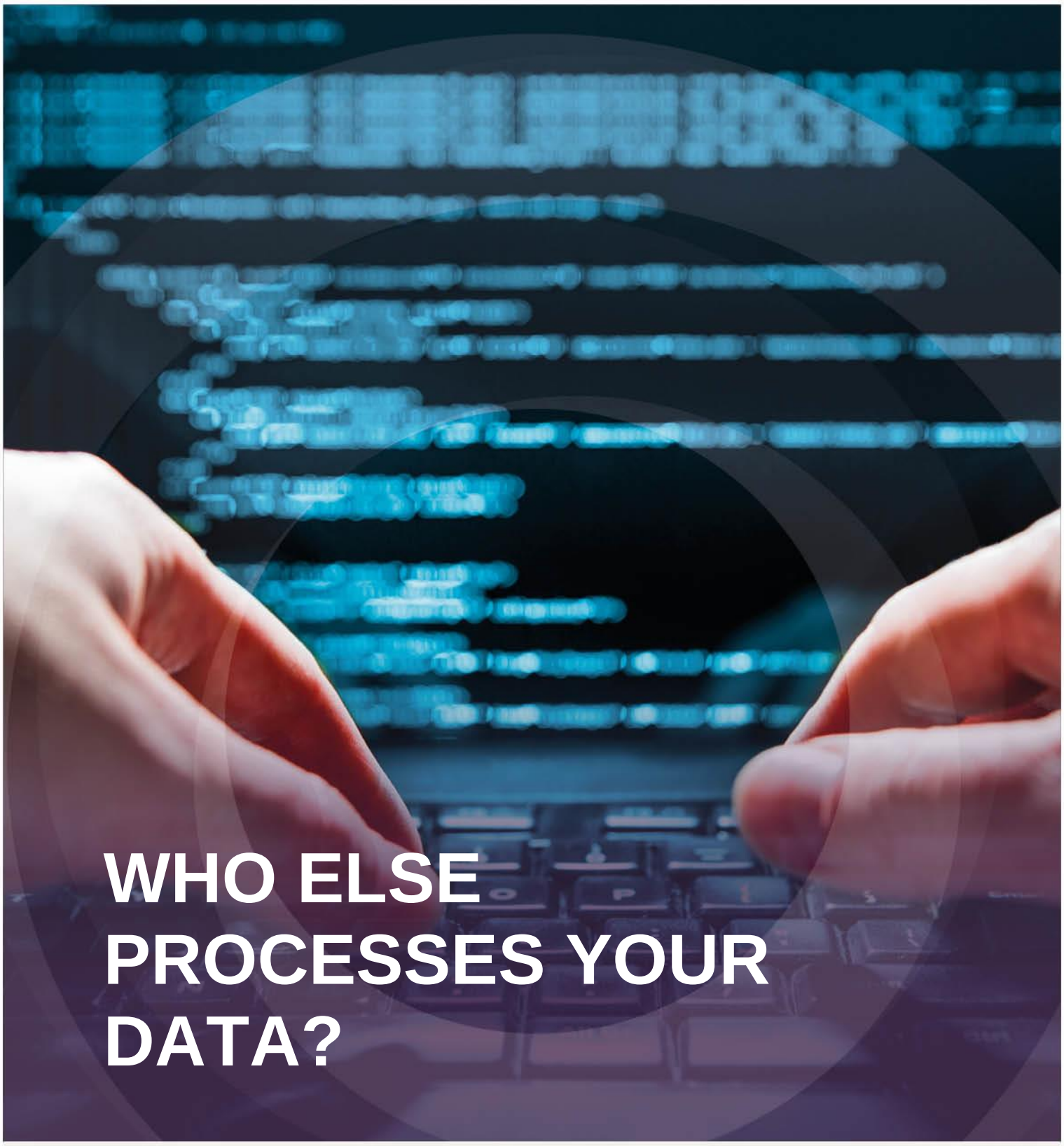
The results of your data mapping exercise will only be as good as the questions that you ask. You might find it useful to think about your legal duties under the GDPR and design your questionnaire so that the responses will help you comply with these legal duties.

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.



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.

WHAT DECISIONS WILL YOU NEED TO TAKE?

GETTING READY FOR THE GDPR

PART FOUR

LEGAL ISSUES AND TRUSTEE DECISIONS

GOWLING WLG

LEGAL ISSUES AND TRUSTEE DECISIONS

As data controllers, pension scheme trustees will need to consider a range of issues and take some important decisions. The most important of these decisions is to decide what legal grounds they have for processing their scheme's personal data.

KEY POINTS

Trustees will need to take some important decisions

As data controllers, trustees are ultimately responsible for the processing of their scheme's personal data. They will need to take decisions on important issues such as the legal grounds for processing the scheme's personal data.

Trustees will need to document their decision making

One of the important overriding principles set out in the GDPR is accountability. Trustees will need to demonstrate: (a) that they have complied; and (b) how they have complied. For decision making, this means keeping records of how decisions were reached.

Trustees will need to establish the legal grounds for processing

Processing personal data is only lawful under the GDPR if one or more of six legal grounds applies. Trustees will need to determine the legal grounds for the processing of the scheme's personal data.

Trustees will need to think about sensitive personal data

There is a general prohibition against the processing of personal data. There are a range of exceptions to this general prohibition, and trustees will need to determine which exceptions apply in order to continue to process sensitive personal data.

What sort of decisions will trustees need to take?

As data controllers, Trustees will need to take important decisions on a range of issues relating to data protection. For example, many trustees will need to consider:

- what are the legal grounds for processing my scheme's personal data?
- what is the exception that will allow me to process sensitive personal data?
- do we need to appoint a data protection officer (DPO)?
- how long do we keep the scheme's personal data for? Will this need to change under the GDPR?

- if we choose not to delete some of the scheme's personal data, should we at least remove it from online and office-based systems into secure archives?
- what should we put in the scheme's privacy notices? Who do we need to send these notices to and when do we need to send them?
- does my scheme have a data protection policy? Does it need to be reviewed and updated? If we don't have a policy, do we need to adopt one?
- how do we share information with employers and related third parties? Do we have an information sharing agreement? If not, do we need to adopt one?

Trustees will also need to document their decision making process and ensure that they have a written record so that they can demonstrate compliance and accountability.

This chapter of the Guide focuses on the legal grounds for processing, but also sets out some guidelines that will apply for trustees approaching any decisions on data protection.

Why are the legal grounds for processing so important for trustees to get right?

Under the GDPR, processing of personal data is only lawful if one or more of legal grounds (also referred to as lawful bases) applies. The ICO has been clear on the importance for data controllers of determining the correct legal ground(s) for processing personal data.

> "You must determine your lawful basis before you begin processing, and you should document it. Take care to get it right first time - you should not swap to a different lawful basis at a later date without good reason."
>
> *Guide to the General Data Protection Regulation* (Information Commissioner's Office)

What are the legal grounds for lawful processing of personal data?

There are six legal grounds set out in the GDPR. Most of them will not, however, apply in the context of private sector occupational pension schemes. Necessary is used repeatedly in the legal grounds, which serves as a reminder of the GDPR's principle of data minimisation.

Consent

Data subject has provided **consent** for **one or more specific purposes** of data processing.

Contract

The processing is necessary for the performance of a contract to which the data subject is party.

Legal obligation

The processing is necessary for compliance with a legal obligation to which the controller is subject.

Vital interests

The processing is necessary in order to protect the vital interests of the data subject or of another natural person.

Public interest

The processing is necessary for the performance of a task carried out in the public interest.

Legitimate interests

The processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party. This ground is subject to a balancing test (see *What is the legitimate interests balancing test* below).

Which of the legal grounds will apply for private sector occupational pension schemes?

Trustees will need to review their scheme's personal data and the processing activities that take place. They may also seek professional advice before taking a decision.

It is clear, however, that trustees of private sector occupational pension schemes will not be able to rely on all of the legal grounds.

Consent is unlikely to be a practical ground for the general processing of pension scheme's personal data (although it might continue to play a role in the processing of sensitive personal data – see *Exemptions for processing sensitive personal data* below).

Contract-based pension providers may process on the legal ground that it is necessary for the performance of the contract, but this is unlikely to be as useful for trust-based pension arrangements.

Similarly, private-sector pension schemes will not typically be able to rely on the legal ground of carrying out tasks in the public interest or protecting vital interests.

This leaves compliance with a **legal obligation** and **legitimate interests**.

Processing is necessary for compliance with a legal obligation

Under the GDPR, data controllers can process personal data if such processing is necessary for compliance with a legal obligation. The ICO has, in its *Guide to the General Data Protection Regulation (GDPR)*, confirmed that this ground can apply if "you need to process the personal data to comply with a common law or statutory obligation".

Pension trustees have a wide range of common law and statutory obligations. A lot of the scheme's personal data is processed in order to comply with these obligations.

For example, the trustee's fiduciary duties are set out in trust law, which is part of the common law. When trustees exercise their powers of discretion on a member query, they are expected to do so in line with their fiduciary duties. Amongst other things, this requires the trustees to take account of all of the relevant facts. In order for the trustees to do this, they are likely to need to request, sort, file and review personal data relating to the member. The trustee's legal ground for this processing is that it is necessary for them to comply with a legal obligation.

UK legislation also requires trustees to process personal data. For example, in order to comply with a member's statutory right to request a transfer, the trustee will need to process that member's personal data. Again, this is necessary in order for them to comply with a legal obligation.

Trustees will, however, still need to consider carefully what personal data they process and why they process it. Not all processing is done in order to comply with a legal obligation. In addition, the processing may not be necessary to comply with a legal obligation. If the processing is an unreasonable and disproportionate way of achieving compliance, this legal ground will not apply.

Trustees may therefore decide to take legal advice on what processing activities are necessary for compliance with legal obligations before they decide whether or not this is an appropriate legal ground for the processing of their scheme's personal data.

"Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party …

Legitimate interests provides one of the most flexible legal grounds for the processing of personal data. In order to protect individuals, the GDPR therefore adds additional wording that requires data controllers consider the rights and freedoms of data subjects.

… except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data"

When the full text of Article 6(f) of the GDPR is taken together, it is clear that data controllers need to carry out a balancing test in order to determine whether their legitimate interests are outweighed by risks to individuals. There are three tests that trustees will need to apply in order to determine if the legitimate interests ground can apply in respect of the processing of the scheme's personal data.

What are the tests to apply to determine if legitimate interests can apply?

Purpose test

Are you pursuing a legitimate interest?

For example, the payment of the correct level of pension benefits to the scheme's beneficiaries is a legitimate interest for a pension scheme trustee to pursue.

Necessity test

Is the processing necessary in order for you to pursue your legitimate interest?

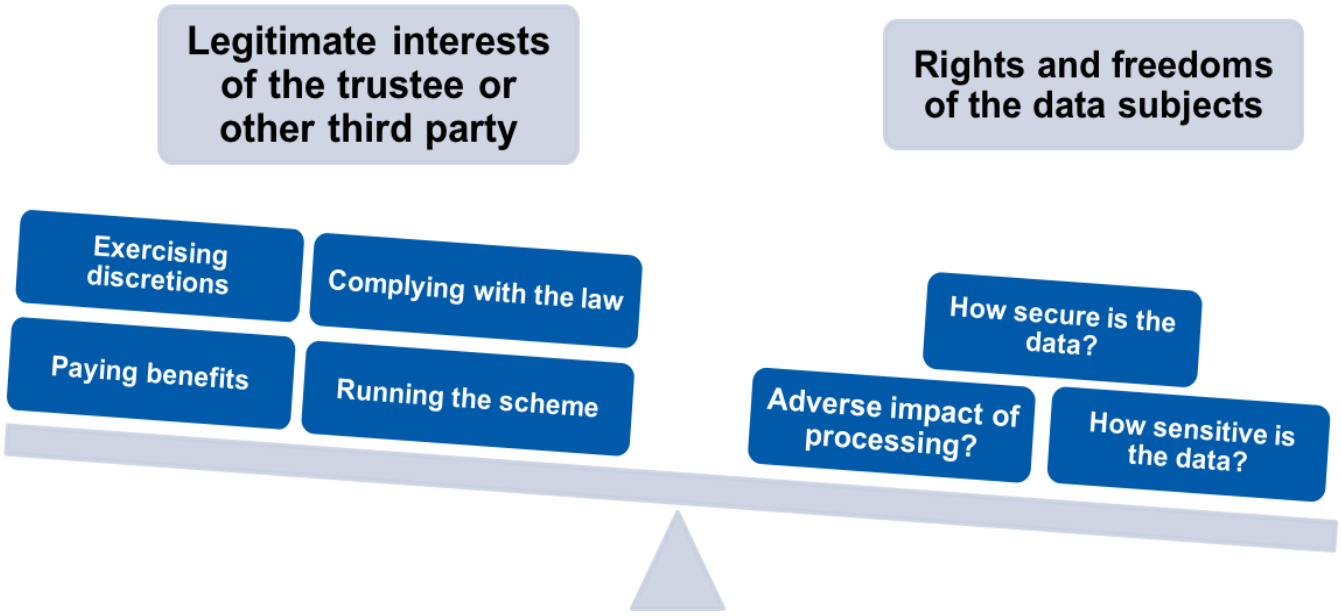
For example, do you need to process the personal data in the way that you do in order to fulfil the purpose? Or, is there a more proportionate or reasonable way of fulfilling the purpose?

Balancing test

Do the individual's interests override the legitimate interest?

As a trustee, you may have determined that you are pursuing a legitimate interest (i.e. the payment of the correct level of pension benefits). You may have also determined that your processing (i.e. the storage and retrieval of bank information) is necessary to fulfil that purpose. But do the individual's interests override the legitimate interest? If you keep the bank information on a secure, password protected system, this is unlikely to be a problem. If, however, you have decided to keep the bank information in an open folder (either online or in the office), then the individual's risk of being a victim of fraud might outweigh your legitimate interests.

Picturing the balancing test for a pensions scheme



Should trustees document legitimate interests?

Trustees should consider their legitimate interests and set them out in writing. They should also consider the rights and freedoms of the data subjects and make sure that these considerations are also set out in writing. In most cases, this should be straightforward – unlike in many online and commercial situations, the interests of trustees and members are more fully aligned. Both parties want to ensure the full and correct payment of benefits to the right people at the right time.

What steps can trustees take to mitigate any risks to individuals?

The rights and freedoms of individuals are far less likely to be infringed if the trustee, as the data controller, takes appropriate data security measures. This might, for example, involve the trustee:

- putting in place or reviewing their scheme's data protection policies;
- applying industry standard data and cyber security measures; and
- ensured that third party service providers and professional advisers also comply with the GDPR.

Can trustees continue to process sensitive personal data?

Under the GDPR, there is a general prohibition on processing of sensitive personal data (called special categories of personal data in the legislation).

For pension scheme trustees, the most common form of sensitive personal data will be medical information. Other forms, such as information revealing race, ethnicity, religious beliefs or trade union membership or data concerning an individual's sexual orientation may also be encountered.

In order to continue to process sensitive personal data, trustees will need to:

Establish a legal ground for processing the personal data + **Determine which exemption applies to override the general prohibition**

What are the exceptions to the general prohibition on the processing of sensitive personal data?

The most relevant exception conditions for trustees of occupational pension schemes are:

- that the individual has provided **explicit and valid consent**
- that the processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of **employment, social security and social protection law**; and
- that the processing is necessary for reasons of **substantial public interest** as authorised by Union or Member State law.

What is explicit and valid consent?

The GDPR sets a high standard for consent, and this is even more important when sensitive personal data is involved. Explicit consent under the GDPR needs to be **clear, freely given, and in writing**. The ICO has stated that consent should be:

> "Consent should be obvious and require a positive action to opt in. Consent requests must be prominent, unbundled from other terms and conditions, concise and easy to understand, and user-friendly.
>
> Consent must specifically cover the controller's name, the purposes of the processing and the types of processing activity."
>
> *Guide to the General Data Protection Regulation* (Information Commissioner's Office)

Consent is likely to remain as an important part of the process of gathering sensitive personal information in respect of ill-health early retirement requests, death benefit decisions and IDRPs. Trustees should, however, ensure that how they obtain and record consent complies with the GDPR and seek legal advice if in doubt. If consent cannot be used, trustees should consider whether any of the other exemptions are available.

When do the other exceptions apply?

There are two exceptions set out in the Data Protection Bill 2017 – 19 that could be useful for trustees of private sector occupational pension schemes:

- employment, social security and social protection law; and
- substantial public interest – occupational pension schemes.

These exceptions are currently being debated as part of the parliamentary process. There are questions as to how they would apply in practice which may be resolved as the Bill progresses. Trustees should seek legal advice as to whether they will apply in their circumstances and may have to wait for the final version of the Data Protection Bill and/or guidance from the ICO.

What about other trustee decisions on data protection issues?

As outlined above, pension scheme trustees will need to consider a wide range of issues relating to data protection and take decisions. The principles set out for establishing legal grounds for processing can be applied to taking other decisions. In particular, trustees should:

Make sure that you understand the issues

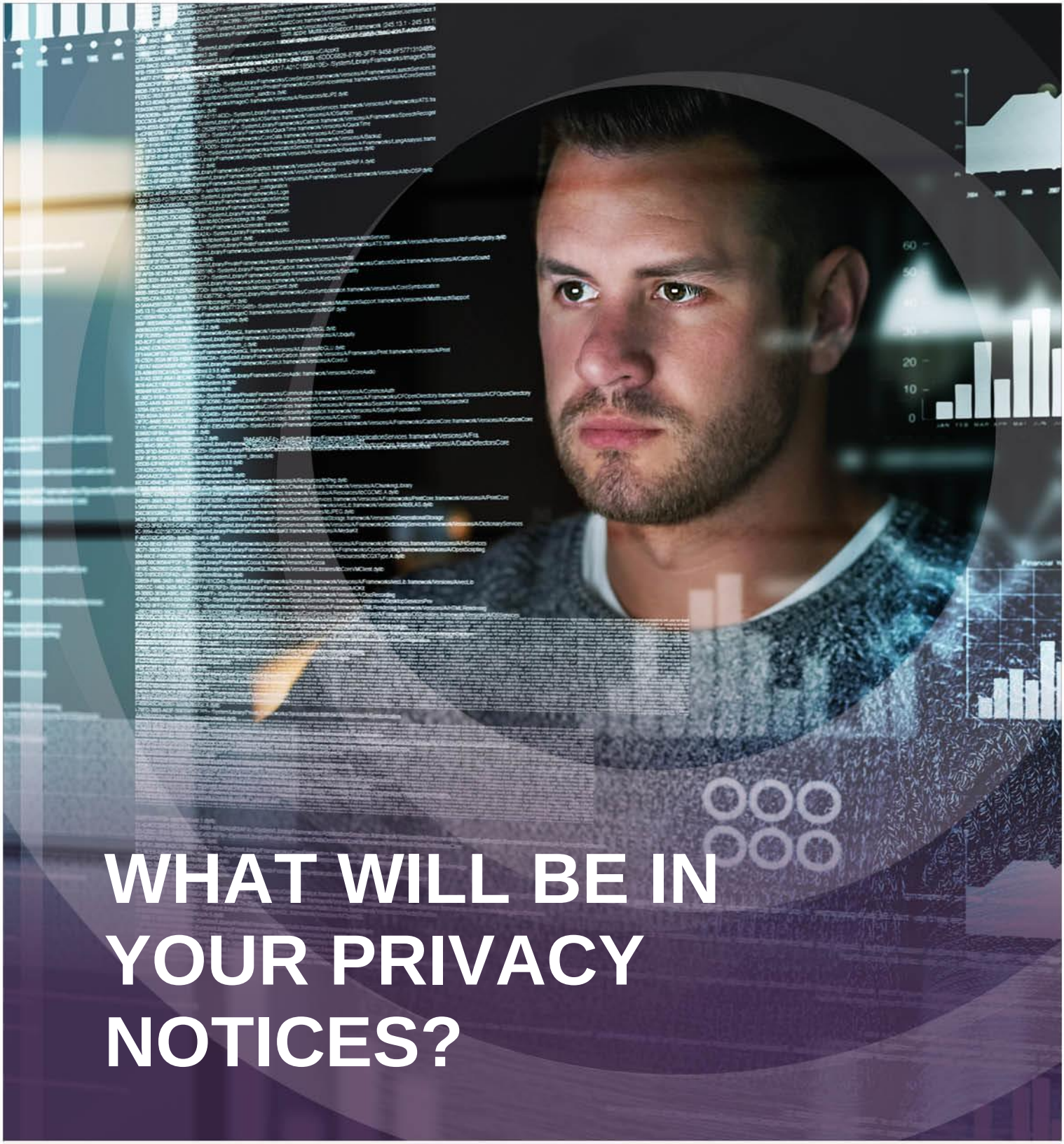
Ensure that you fully understand the issues. This might come from training, such as reading this Guide or attending training sessions or seminars. In addition, the ICO has produced a lot of guidance that can help trustees get to grips with their legal duties as data controllers. Where appropriate, trustees should also seek additional professional advice.

Schedule time for decision making

Make time for discussion and decision making. Trustees will need time to consider the information and make informed decisions. Set aside plenty of time for this at trustee meetings and consider whether having a standalone meeting on data protection would be the most efficient way of dealing with the issues.

Document compliance – that you've complied and how you've complied

Document the decision **and** the decision making process. As part of the principle of accountability, trustees will need to be able to evidence both that they have complied with the law **and** how they have complied with the law. A record of the relevant factors and the steps taken to reach a decision will be helpful if the trustee is challenged in the future.



WHAT WILL BE IN YOUR PRIVACY NOTICES?

GETTING READY FOR THE GDPR

PART FIVE

COMMUNICATING WITH MEMBERS

GOWLING WLG

COMMUNICATING WITH MEMBERS

Data controllers are required to share certain information with individuals whose personal data they process. The GDPR specifies what should be included in this information and how it should be written.

KEY POINTS

Data controllers have to provide information to data subjects

In the pensions context, this will mean trustees issuing information to members and other beneficiaries. These statements are also known as privacy notices or a fair use notices.

Privacy notices must cover specified information

The GDPR sets out the information that must be contained in a privacy notice. This includes general information such as the name and contact details of the data controller along with more detailed information such as the purpose and legal grounds for processing

The style of privacy notices is also specified

The GDPR is keen to ensure that privacy notices are as user friendly and accessible as possible. Trustees will need to issue privacy notices in plain English and ensure that they are intelligible.

Privacy notices have to be issued

Privacy notices have to be issued to data subjects. This means that they have to be actively sent rather than passively displayed. In practice, for schemes that do not primarily communicate online, this is likely to mean sending a letter or email rather than displaying a notice.

What are privacy notices?

Under the GDPR, data controllers are required to provide certain information to individuals whose personal data they process. This information is often referred to as a privacy notice, but may also be called a fair use notice, a data protection notice or a data protection statement.

What form can privacy notices take?

The GDPR does not specify a particular form for privacy notices. The information can be provided in a variety of ways and doesn't have to be set out in a single document or on a single webpage. The ICO has confirmed that privacy notices can be provided:

- orally (e.g. recorded telephone messages or a script that is read out as part of accessing a telephone-based service);
- in writing (e.g. as a printed letter or statement or as a section in a larger document (for example, a section of a member booklet)); and

- electronically (e.g. in text messages, on websites, in emails and in mobile apps).

The ICO has stated that it is good practice to use the same medium that you use to collect personal information to deliver privacy notices. For many pension schemes, this may suggest a printed notice issued to individuals in the post represents good practice.

What should privacy notices include?

In order to comply with the GDPR, privacy notices should set out:

- the identity and contact details of the data controller and, if applicable, the identity and contact details of the data protection officer;
- the legal grounds for the data controller to process the personal data. If one of the legal grounds is that processing is necessary to pursue the data controller's (or a third party's) legitimate interests, the privacy notice should also explain what the legitimate interests are;
- whether the personal data is shared with a third party (this should include details of transfers of personal data outside of the European Union);
- how long the personal data is kept for (or the criteria for determining how long the personal data is kept for);
- each of the data subject rights, including the right to withdraw consent (if applicable) and the data subject's ability to lodge complaints with the ICO; and
- the existence of automated decision making, including profiling.

If the individual has provided their personal data to the data controller (e.g. a pension scheme member has filled in a form and given this to the trustee), the privacy notice should:

- explain whether the personal data is required as part of a statutory or contractual requirement; and
- set out the possible consequences of failing to provide the personal data.

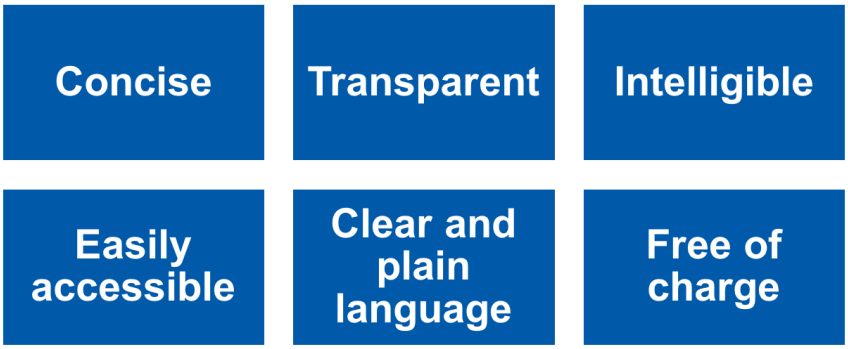
If the individual did not provide their personal data (e.g. it came from another source, such as the member's employer), the privacy notice should:

- explain how the data controller obtained the personal data; and
- set out the categories of personal data that the data controller processes.

Pension schemes have a large amount of personal data that can come from different sources. Trustees may decide to cover all of the required elements so that the privacy notice will apply whether the information came from the individual or from another source.

How should privacy notices be written?

As well as specifying what needs to be in a privacy notice, the GDPR sets out how they should be written. In order to comply with the GDPR, privacy notices should be:



Do trustees have to send privacy notices to members?

There isn't a single right answer that applies to all data controllers – it will depend on:

- how the Trustee usually communicates with its members – if it already has an online platform that handles member queries, the answer will be different to a client that relies on paper-based communication;
- the characteristics of the membership – are the members all online? Do they all have email addresses? Do most of the member still work for the employer?; and
- what the Trustee has already done in respect of privacy statements (including if they have specified that future updates will be provided via an online privacy notice).

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

Draft or review your privacy notice

Privacy notices require a lot of information and it might therefore be more efficient to draft them towards the end of a data protection compliance project. If you already have a privacy notice in place, you'll need to review it in order to confirm that it meets all the requirements set out in the GDPR.

Determine whether any third parties will be covered by your privacy notice

As part of their data mapping process, trustees should have identified any third parties who are joint controllers in respect of the scheme's personal data. Trustees should consider whether these third parties need to be included in the scheme's privacy notice.

Decide when you will send your privacy notice and how you will send it

Many pension scheme trustees will issue privacy notices by sending a letter or email to members. If there is already a communication being planned, can the privacy notice be included as part of that communication?

Determine how you will update the privacy notice if there are material changes

Privacy notices may need to be updated in the future. If the trustee has indicated that future updates will be made to an online privacy notice, it will be a lot easier for updates to be made to the online version rather than sending hard copy versions.

DATA PROTECTION TERMS AND PHRASES

A GLOSSARY OF TERMS AND PHRASES USED IN THE GENERAL DATA PROTECTION REGULATION

DATA PROTECTION TERMS AND PHRASES

KEY WORD OR PHRASE	WHAT THE KEY WORD OR PHRASE MEANS
Data controller	means the natural or legal person or other body who, alone or jointly with others, determines the purposes and means of the processing of personal data. This means that the data controller exercises overall control over the 'why' and 'how' of a data processing activity.
Data Protection Act 1998	is the legislation that currently applies to the processing of personal data in the UK. The Data Protection Bill 2017 – 19 will repeal the Data Protection Act 1998.
Data Protection Bill 2017 – 19	is new UK primary legislation that will complement the General Data Protection Regulation and which sets out detail on the exemptions to the general prohibition on the processing of special categories of personal data.
Data Protection Legislation	means the Data Protection Act 1998, the Data Protection Bill 2017 – 19 and the General Data Protection Regulation, together with regulatory guidance issued by the European Commission (via the Article 29 Working Party) and the Information Commissioner's Office.
Data protection principles	means the principles that are set out in the Data Protection Legislation relating to the processing of personal data. In the General Data Protection Regulation, there are six principles: • lawfulness, fairness and transparency; • purpose limitation; • data minimisation; • accuracy; • storage limitation; and • integrity and confidentiality. • In addition, there is an overarching principle of accountability.
Data processor	means a natural or legal person or other body who processes personal data on behalf of the data controller.

Data subject	means the identified or identifiable living individual to whom personal data relates.
General Data Protection Regulation (GDPR)	is the primary EU legislation that, on and from 25 May 2018, will apply to the processing of personal data in all member states of the EU.
Information Commissioner's Office (ICO)	is the UK's national data protection authority. It is a public body that is charged with regulating information rights, public sector transparency and individual's privacy in the UK.
Privacy notice	means the information that is provided to inform individuals about what you do with personal data. Under the Data Protection Legislation, data controllers must provide accessible information to individuals about the use of their personal data.
Processing	means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Personal data	means any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number etc.
Special categories of personal data (also referred to as sensitive personal data)	means: • personal data that is personal data which reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership; and • the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person; • data concerning health; or • data concerning a natural person's sex life or sexual orientation.
Technical and organisational measures	means the steps that are taken by a data controller in order to ensure and to be able to demonstrate that processing is performed in accordance with the GDPR. The GDPR does not specify which measures are required, but it does highlight pseudonymisation as a method of increasing the security of personal data.

FIND OUT MORE

Gowling WLG's pensions team has a specialist group focusing on data protection issues in the run up to the GDPR going into effect. They bring together extensive trustee, employer and industry expertise along with experience of dealing with data protection issues in practice. Please contact any of us for more information on how we can work together to solve your data protection issues.

Jason Coates

Partner

T 020 3636 7886
jason.coates@gowlingwlg.com

Jason Coates is a leading UK pensions lawyer. He helps his clients to respond to the challenges and opportunities they face in operating their pension arrangements, commercially and without jargon.

His clients include trustees of UK-based pension schemes, whether defined benefit, defined contribution or hybrid schemes, corporates in all sectors with defined benefit pension schemes, companies in all sectors who need help establishing and running retirement arrangements, and other law firms who need high quality UK pensions advice for their clients on complex deals.

Paul Feathers

Partner

T 020 3636 7952
paul.feathers@gowlingwlg.com

Paul Feathers is a partner who focuses on risk transfer and investment issues as part of a general pensions law practice. He has a reputation as a "no-nonsense" lawyer who is pragmatic and commercial in his approach, using the law as a tool to help clients to achieve their goals rather than as a barrier to doing so.

Paul is a go to lawyer for clients who want to work with someone who will tell it as it is in plain English, and who is focussed at every step on delivering a solution that works for his clients without exposing them to unacceptable risk.

Ian Chapman-Curry

Head of Pensions Excellence

T 020 3636 7870
ian.chapman-curry@gowlingwlg.com

Ian works at the forefront of legal developments, including workplace pension reform, pension flexibilities, Brexit and data protection. He has worked for the DWP, NEST and Wm Morrison Supermarkets to develop solutions for complex automatic enrolment problems. He is currently implementing practical data protection solutions that are as easy and cost effective as possible.

Stephen Longfellow

Principal Associate

T 020 3636 8007
stephen.longfellow@gowlingwlg.com

Stephen Longfellow is a London based principal associate. He advises trustees and employers on all aspects of pensions law, helping them to navigate the complex and ever changing pensions landscape. Stephen's clients benefit from his broad experience and thorough understanding of technical legal issues which he converts into clear, practical advice.

GOWLING WLG (UK) LLP
T +44 (0)370 903 1000
gowlingwlg.com

GOWLING WLG