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?

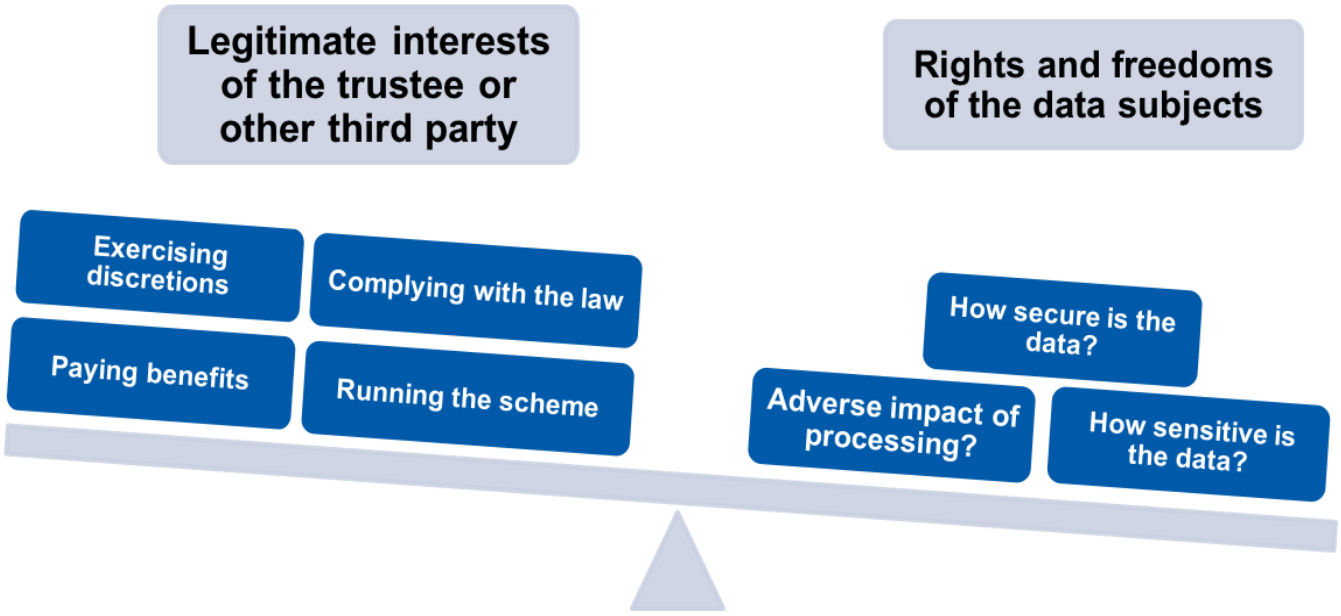
For example, do you need to process the personal data in the way that you do in order to fulfil the purpose? Or, is there a more proportionate or reasonable way of fulfilling the purpose?

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.