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.

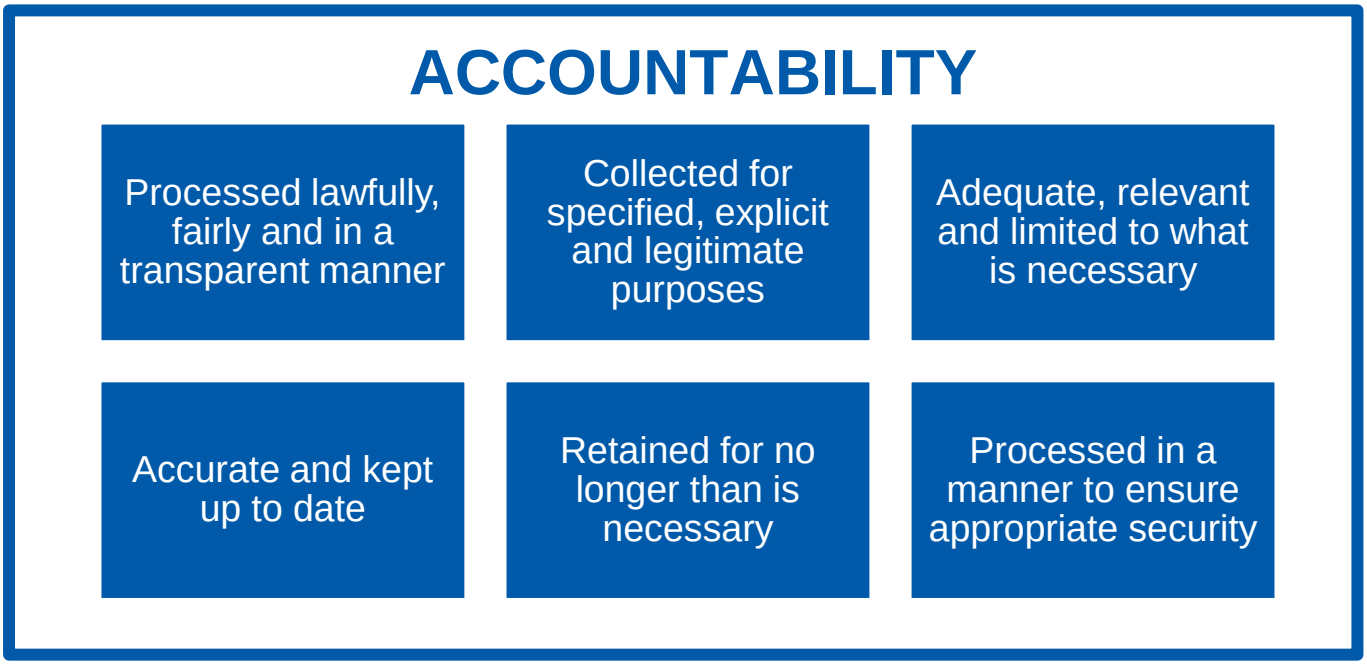
In the pensions industry, this means that data protection issues will be more central to negotiations on contracts and are likely to feature more prominently on everyone's list of priorities. In addition, it is likely that employers will be more concerned to ensure that trustees are complying with their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