Sackers

# Data Protection – the new requirements

**Alert** | 04 April 2017

## Introduction

The General Data Protection Regulation (GDPR) promises a major shake-up of European data privacy laws when it comes into effect on 25 May 2018.

Trustees, employers and pension providers should start preparing now as, despite Brexit, the Government has confirmed that the GDPR will apply in the UK from that date.

## Key points

- The main aim underpinning the GDPR, which will apply from 25 May 2018, is to create a unified regulatory data protection regime that is fit for the digital age.
- Whilst many of the GDPR's requirements are similar to existing data protection provisions, the new rules will strengthen data protection requirements by introducing new contractual obligations, increasing the amount of information that needs to be given to individuals, enhancing reporting obligations in the event of a breach and imposing heavier sanctions for non-compliance.
- The Information Commissioner's Office (ICO) is pressing ahead with its plans to produce guidance on the new requirements. A consultation on consent under the GDPR closed on 31 March 2017, whilst draft guidance on contracts and liability is expected "early in 2017".
- Trustees, employers and providers should be preparing now, so that they are ready for the new data protection requirements in advance of May 2018.

## What's new?

- **Sanctions:** The maximum penalties for non-compliance with the GDPR will increase significantly – from £500,000 currently, to the greater of €20,000,000 or 4% of an organisation's global turnover.
- **Contractual provisions:** Contracts will need to include specific additional wording as to how data should be stored and protected.

- **Information to individuals:** Individuals will need to be provided with additional information at certain key junctures. For example, when "personal data" (see below) is collected from an individual, they will need to be told how long this data will be stored for.

- **Reporting breaches:** Serious data breaches will need to be reported to the ICO within 72 hours where feasible, and to individuals if their interests would be affected by the breach. An example of a serious data breach is one that results in the loss of or unauthorised disclosure of data, unless this is unlikely to be a risk to the affected individuals' rights and freedoms.

- **Right to be forgotten:** The GDPR gives individuals stronger rights to require that personal data held about them is removed.

- **Data protection officer:** Organisations will be required to appoint a data protection officer if their core activities require "regular and systematic monitoring of data subjects on a large scale". This is not likely to affect most occupational pension schemes but could potentially affect providers.

- **Consent:** The GDPR introduces more stringent requirements on how individuals should give their consent to data processing. Consent will have to be "freely given, specific and informed" and, once given, can be withdrawn at any time.

# A new twist on current concepts

The GDPR imposes new obligations on both "data controllers" and "data processers", so it is important to understand who each is in relation to a pension scheme.

## Who is a data controller?

Data controllers are responsible for ensuring that any personal data is processed in a manner which complies with relevant requirements (currently, the Data Protection Act 1998, DPA). In the context of a pension scheme, this will include the trustees. If this obligation is not met, then a data controller potentially risks enforcement action (including prosecution) by the ICO and compensation claims from individuals.

Currently, data controllers who are processing personal information have to register with the ICO, unless an exemption applies. As this requirement did "not in all cases contribute to improving the protection of personal data", the GDPR contains no equivalent provision.

Instead, organisations must be able to demonstrate that they comply with the GDPR. For example, when using new technologies and new types of processing operation, a "data protection impact assessment" may need to be carried out in order to assess potential risks.

As regards joint data controllers (which may include employers and scheme administrators alongside trustees, depending on how data is being used), the GDPR creates a stronger joint liability framework. For example, it:

- requires joint controllers to set out their responsibilities "in a transparent manner", a summary of which should be made available to individuals on whom data is held

- makes clear that joint controllers are each fully liable for any damage resulting from a breach of the GDPR, unless a controller can show that it is not in any way responsible.

## Who is a data processor?

A data processor is someone (other than an employee of the data controller) who processes personal data on behalf of the data controller. In the pensions context, scheme administrators (and possibly payroll providers) will be data processors.

For the first time, data processors will have direct obligations under the GDPR, which means that they too can be fined if things go wrong.

Appropriate contracts should be in place recording obligations in relation to the security of the personal data held and where liability lies if things go wrong. A number of new features will need to be covered by a contract, including that the processor will only process personal data in accordance with the data controller's documented instructions and that it will help ensure that the data controller's obligations are met.

## What is personal data?

Under the GDPR, "personal data" means any information relating to a "natural person" (namely, the individual on whom data is held) which enables that individual, whether directly or indirectly, to be identified. Personal data therefore includes someone's name, NI number or other factors which are specific to their identity, including physical, cultural or social factors.

# Lawful processing

Trustees need to determine the basis on which the data they hold is processed. For data processing to be lawful, it must meet at least one of six conditions, to which Member States can also add their own.

Conditions relevant to pension schemes include:

- the processing is necessary for the purpose of legitimate interests pursued by the data controller or a third party (such as the effective running of the pension scheme by the trustees and scheme administrator)
- the member having given their consent to the processing of their data for one or more specific purposes
- the processing being necessary for the performance of a contract, for example, to pay benefits due under the scheme.

# Actions for trustees (and other data controllers)

## Review existing systems and processes

Steps for now include:

- carrying out an audit of existing data so as to check what data is held, why it is being held, how long it has been held for, and whether it is still needed
- assessing the legal basis on which the data is held
- looking at the way in which data is held and processed, and the circumstances in which it may be disclosed to others
- getting legal advice on what changes may be needed to existing contracts or new contracts being put in place.

# How we can help

We will be producing a series of Alerts on the different elements of the GDPR in the countdown to May 2018. We can also help trustees get ready now for the GPDR in any number of ways, including:

- identifying the key questions to address so as to audit your current data
- reviewing existing or new contracts
- considering the policies and procedures you may need to put in place or update.

For assistance with the above, or any other GDPR help you may need, please speak to your usual Sackers contact.

Sacker & Partners LLP
20 Gresham Street
London EC2V 7JE
T +44 (0)20 7329 6699
E enquiries@sackers.com
www.sackers.com