FYI®
For Your Information®
UK

Volume 2017 | Issue 60 | 1 September 2017

GDPR and Pension Schemes: Controllers and Processors (Responsibilities)

The General Data Protection Regulation (GDPR) sets out the responsibility and liability requirements of both data controllers and processors. A new accountability principle requires controllers to be responsible for, and be able to demonstrate compliance with the principles. Additionally, under the present data protection requirements, a data processor is liable to its data controllers only under the terms of the contract between them. Under the GDPR, data processors will have direct obligations to comply with the GDPR and will be directly liable to compensate individuals for loss caused by any breaches.

This is the first in a series of six briefing notes about the GDPR that takes effect in the UK from 25 May 2018.

Controllers

Definition
'Controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purpose and means of the processing of personal data.

Responsibility

The data controller must implement and keep under review appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with the GDPR. This should take into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of individuals (i.e. a risk register).

This should also include an appropriate data protection policy (where proportionate in relation to processing activities). This may involve adherence to codes of conduct approved by the Information Commissioner's Office.

Joint controllers

Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers. They need to determine their respective responsibilities for compliance with the GDPR, in particular as regards the exercising of the rights of individuals and their duties to provide privacy notices. It should be

noted that individuals are able to exercise their rights in respect of and against each of the controllers separately.

Processors

Definition
'Processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

What does processing entail?
'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.

Obligations

The present data protection requirements require controllers to confirm that their processors have adequate data security. Under the GDPR, controllers are required to only use processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of the GDPR and ensure the protection of the rights of individuals.

Engagement of another processor will only occur with the prior specific or general written authorisation of the controller. Where the latter applies, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, giving the controller the opportunity to object to such changes.

Where a processor engages another processor for carrying out specific processing activities on behalf of the controller, the same data protection obligations as set out in the contract shall be imposed on that other processor. Where the other processor fails to fulfil its data protection obligations the initial processor shall remain fully liable to the controller for the performance of that other processor's obligations.

The list of obligations that controllers must place on processors is greatly expanded in the GDPR. Processing contracts setting out obligations must be in writing, which can be in electronic form. The contract must contain a description of the scope, nature and purpose of processing, the duration of the processing and the types of personal data and categories of individuals whose data is being processed.

What obligations shall the processing contract stipulate?
Process the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a country outside the European Economic Area (EEA).
Ensure that persons authorised to process the personal data have committed themselves to confidentiality.
Ensure that appropriate technical and organisation measures are taken to ensure a level of security appropriate to the risk.
Assist the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the individual's rights.
Assist the controller in ensuring compliance with the obligations in relation to security of processing, data breaches and data protection impact assessments.

What obligations shall the processing contract stipulate?
At the choice of the controller, deletion or return of all the personal data to the controller after the end of the provision of services relating to processing, and deletion of existing copies (unless storage is required by EU law or Member State law (but not foreign law such as US law)).
Make available to the controller all information necessary to demonstrate compliance with these obligations and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.

Records of Processing Activities

Controllers are required to maintain a record of processing activities under its responsibility. Additionally, processors are required to maintain a record of all categories of processing activities carried out on behalf of a controller. The records have to be in writing, including in electronic form.

These obligations do not apply where the organisation employs fewer than 250 persons, however, where the processing:

- is likely to result in a risk to the rights and freedoms of individuals
- is not occasional, or
- includes special categories of data or personal data relating to criminal convictions and offences

the 250 person requirement is disregarded.

Controllers records of processing activities

What information (where applicable) shall the records contain?
Name and contact details of the controller and (where applicable) the joint controller, their representative(s) and the data protection officer.
Purposes of the processing.
Categories of individuals and categories of personal data.
Categories of recipients to whom the personal data has been or will be disclosed, including recipients in countries outside the EEA.
Transfers of personal data to countries outside the EEA and the safeguards in place.
Where possible, the envisaged time limits for erasure of the different categories of data.
Where possible, a general description of the technical and organisational security measures taken to ensure a level of security appropriate to the risk.

Processors records of processing activities

What information (where applicable) shall the records contain?
Name and contact details of the processor(s) and of each controller on behalf of which the processor is acting and (where applicable) their representative(s) and the data protection officer.
Categories of processing carried out on behalf of each controller.
Transfers of personal data to countries outside the EEA and the safeguards in place.

What information (where applicable) shall the records contain?
Where possible, a general description of the technical and organisational security measures taken to ensure a level of security appropriate to the risk.

Impact on Pension Schemes

Processors (like pension scheme administrators) will be directly liable to members if the member suffers loss from the processor's breach of the GDPR requirements.

Scheme actuaries (of defined benefit pension schemes) are usually considered to be joint data controllers with the scheme trustees and are likely to be subject to the same requirements as trustees.

Trustees (and scheme actuaries) and pension scheme administrators will be subject to the record keeping requirements and should be able to demonstrate to the Information Commissioner's Office (or other supervisory authority) compliance (i.e. accountability) on request.

Recommended Actions for Employers and Trustees

- Identify all service providers or suppliers and ask them what they are doing to prepare for GDPR.
- Review and renegotiate, where appropriate, contracts between trustees and/or employers and service providers.
- Engage with the scheme actuary and determine how the GDPR will impact on their duties.
- Review the pension scheme's risk register and consider the controls that are in place to mitigate the risks raised by the new GDPR requirements.
- Identify what categories of personal data are being processed and the categories of individuals the data relates to (i.e. prepare a data mapping record).
- Liaise with all service providers to ensure that they are also keeping records of processing activities.
- Review all records to determine whether these comply with the GDPR, update as necessary, ensuring that training is given to appropriate people.

Further Reading

- Information Commissioner's Office (ICO): Overview of the GDPR
- ICO: Draft consent guidance for public consultation
- FYI: Preparing for the GDPR
- FYI: GDPR and Pension Schemes: Lawful Basis for Processing
- FYI: GDPR and Pension Schemes: The Right to Be Informed
- FYI: GDPR and Pension Schemes: Rights of Individuals
- FYI: GDPR and Pension Schemes: Personal Data Breaches and Penalties
- FYI: GDPR and Pension Schemes: Transfers Outside the European Union

Types of Personal Data

Personal data	Special categories of personal data ('sensitive data')	Pseudonymous data
This is any information relating to a living individual who can be identified (directly or indirectly) by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person. The definition is more expansive than that under the Data Protection Act 1998, reflecting changes in technology (e.g. an IP address is deemed to be personal data).	This replaces the current definition of sensitive personal data, but is essentially the same. It would include: • personal data that reveals racial or ethnic origin, political opinions, religious beliefs, trade union membership • genetic data (inherited or acquired genetic characteristics) • biometric data (specific technical processing relating to physical, physiological or behavioural characteristics) • data concerning a person's physical or mental health (including the provision of health care services, which reveal information about health status) • data concerning a person's sex life or sexual orientation. The GDPR generally prohibits processing of this personal data without the individual's explicit consent.	This is a new category of data. The personal data is processed in such a manner that it cannot be attributed to a specific individual without the use of additional information. The additional information must be kept separately and subject to technical and organisational measures to ensure the data is not attributed to an identified or identifiable person.

Authors
Nikki Williams, Senior Technical Consultant
Gary Crockford, Technical Services Manager

Produced by the Knowledge Resource Centre
The Knowledge Resource Centre is responsible for national multi-practice compliance consulting, analysis and publications, government relations, research, surveys, training, and knowledge management. For more information, please contact your consultant or call us on 0800 066 5433.

CONDUENT