

GDPR and Pension Schemes: Rights of Individuals

In addition to the right to information (privacy notices) there are seven other rights that individuals have under the General Data Protection Regulation (GDPR). These are: right of access, right to rectification, right to erasure (right to be forgotten), right to restriction of processing, right to data portability and right to object to processing (where the lawful basis of processing is in the public interest or legitimate interest) and right not to be subject to a decision based solely on automated processing.

The right to be forgotten and the right to data portability are new rights. Subject access rights are to be free of charge (rather than a £10 fee under the Data Protection Act 1988 (DPA)) and requests have to be met within one month of receipt (rather than 40 days).

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

In this issue: [Rights of Individuals](#) | [Impact on Pension Schemes](#) | [Recommended Actions for Employers and Trustees](#) | [Further Reading](#) | [Types of Personal Data](#)

Rights of Individuals

The Right of Access (subject access requests)

This is the right for individuals to access their personal data so that they are aware of and can verify the lawfulness of the processing. The first copy of the information must generally be provided free of charge, although a reasonable fee (based on the administrative cost of providing the information) may be charged for further copies requested by the individual or when a request is manifestly unfounded or excessive, particularly if it is repetitive. The information must be provided without delay and at the latest within one month of receipt, unless the request is complex or a large number of requests have been made when this period can be extended by a further two months.

The identity of the person making the request must be verified using 'reasonable means' and if the request is made electronically (i.e. by email), the information should be provided in a commonly used electronic format, unless the individual requests otherwise. Where possible, organisations should be able to provide remote access to a secure self-service system which would provide the individual with direct access to the information.

What information has to be supplied with the personal data?

The purposes of the processing.

The categories of personal data concerned.

The recipients or categories of recipient to whom the personal data has been or will be disclosed, in particular recipients in countries outside of the European Economic Area (EEA). Where it is transferred to a country outside of the EEA, details of the appropriate safeguards.

Where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period.

The existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the individual or to object to such processing.

The right to lodge a complaint with a supervisory authority (i.e. the Information Commissioner's Office in the UK).

Where the personal data is not collected from the individual, any available information as to their source.

The existence of automated decision-making, including profiling.

The Right to Rectification

This is the right for individuals to obtain from the controller without undue delay the rectification of inaccurate personal data. Taking into account the purposes of the processing, the individual shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

Where the personal data has been disclosed to other recipients, the controller shall let them know of the rectification (unless this proves impossible or involves disproportionate effort).

The Right to Erasure (right to be forgotten)

This is the right for individuals to obtain from the controller the erasure or deletion of personal data without undue delay, although this is not an absolute right to be forgotten. For instance, where the processing is required to comply with a legal obligation, or for the establishment, exercise or defence of legal claims, the controller is exempted from the obligation.

Where the personal data has been disclosed to other recipients, the controller shall let them know of the erasure (unless this proves impossible or involves disproportionate effort).

What grounds must apply for the controller to be obliged to erase personal data?

The personal data is no longer necessary in relation to the purposes for which it was collected or otherwise processed.

The individual withdraws consent where there is no other legal ground for the processing.

The individual objects to the processing and there are no overriding legitimate grounds for the processing.

The personal data has been unlawfully processed.

The personal data has to be erased for compliance with a legal obligation.

The personal data has been collected in relation to the offer of information society services to a child.

The Right to Restrict Processing

This is the right for individuals to obtain from the controller restriction of processing. Essentially, this means that the personal data can be stored, but only processed with the individual's consent, or for the establishment, exercise or defence of legal claims, or for the protection of the rights of another individual or legal entity.

Where the personal data has been disclosed to other recipients, the controller shall let them know of the restriction of processing (unless this proves impossible or involves disproportionate effort).

What grounds must apply for the controller to be obliged to restrict the processing of personal data?

The accuracy of the personal data is contested by the individual, for a period enabling the controller to verify the accuracy of the personal data.

The processing is unlawful and the individual opposes the erasure of the personal data and requests the restriction of their use instead.

The controller no longer needs the personal data for the purposes of the processing, but they are required by the individual for the establishment, exercise or defence of legal claims.

The individual has objected to processing (where it was necessary for the performance of a public interest task or purpose of legitimate interests) and the controller is verifying whether their legitimate grounds override those of the individual.

The Right to Data Portability

This is the right for individuals to receive personal data that they have provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit the data to another controller without hindrance from the controller, where technically feasible. It only applies where the processing is based on the individual's consent or for the performance of a contract and the processing is carried out by automated means.

The Right to Object

This is the right for individuals to object to: processing of personal data based on legitimate interests or the performance of a task in the public interest / exercise of official authority (including profiling); direct marketing; and processing for purposes of scientific / historical research and statistics.

Rights Related to Automated Decision-Making Including Profiling

This is the right for individuals not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects or similarly significant effects on the individual.

Impact on Pension Schemes

Right of access

Pension schemes already have to comply with subject access requests under the DPA. The information to be given has been extended, the timescales shortened and it now, generally, has to be given free of charge.

Right to rectification

Pension schemes have a duty to ensure their data is as correct and complete as possible and will often ask members to check the information provided in benefit statements etc. so the right to rectify should have no additional impact on the pension scheme.

Right to erasure

Pension schemes would find it very difficult to manage without members' personal data and in most situations members would not ask for their personal data to be erased as this would result in difficulties in receiving benefits either on retirement or on death. This is also why using consent as the lawful basis for processing data would not be the most appropriate basis for pension schemes.

However, in cases where a member has to provide trustees with medical information about their ill-health in order to be considered for an ill-health early retirement pension, explicit consent is likely to be given. Also, on a member's death, potential beneficiaries will be asked to provide trustees with information about the deceased member's personal relationships in order to be considered for lump sum death benefits and/or dependants' pensions or children's allowances. These individuals may ask for these special categories of personal data (e.g. sexual orientation) to be erased.

Right to restrict processing

Pension schemes are unlikely to receive requests from individuals to restrict the processing of their personal data. However, it may be of use where the controller (and pension scheme administrators) may wish to retain the data in case of legal claims in the future but has no intention of processing the data. This may require system changes.

Right to data portability

Pension schemes are unlikely to receive requests from individuals to have the personal data that they have supplied to be transferred to another controller.

Right to object

Pension schemes are unlikely to receive such requests from individuals.

Rights related to automated decision-making including profiling

Pension schemes are unlikely to make decisions based on automated processing.

Recommended Actions for Employers and Trustees

- Determine the lawful basis for processing personal data in all circumstances, particularly ill health, for expression of wish forms, and from potential beneficiaries following a member's death.
- Document the reasons for determining the lawful basis so that this can be explained if challenged.
- Consider whether members or beneficiaries (or anyone whose personal data may be held) may make a subject access request and how this may impact on the pension scheme.
- Establish or review and update any procedures to comply with these requests including retaining records.
- Consider how and whether information can be given online.
- Consider how to respond to a request to erase or restrict the processing of personal data.
- Be aware of the rights of rectification, data portability, objection and automated decision-making.

Further Reading

- Information Commissioner's Office (ICO): [Overview of the GDPR](#)
- ICO: [Privacy notices code of practice](#)
- FYI: [Preparing for the GDPR](#)

- FYI: [GDPR and Pension Schemes: Controllers and Processors](#)
- FYI: [GDPR and Pension Schemes: Lawful Basis for Processing](#)
- FYI: [GDPR and Pension Schemes: The Right to Be Informed](#)
- 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
<p>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.</p> <p>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).</p>	<p>This replaces the current definition of sensitive personal data, but is essentially the same. It would include:</p> <ul style="list-style-type: none"> • 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. <p>The GDPR generally prohibits processing of this personal data without the individual's explicit consent.</p>	<p>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.</p>

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.

This publication is for information only and does not constitute legal advice; consult with legal, tax and other advisors before applying this information to your specific situation.

Conduent HR Services is a trading name in the UK for Buck Consultants Limited (registered number 1615055), Buck Consultants (Administration & Investment) Limited (registered number 1034719), and Buck Consultants (Healthcare) Limited (registered number 172919), which are private limited liability companies registered in England and Wales. All have their registered office at 160 Queen Victoria Street, London EC4V 4AN. Buck Consultants (Administration & Investment) Limited and Buck Consultants (Healthcare) Limited are authorised and regulated by the Financial Conduct Authority.

© 2017 Conduent Business Services, LLC. All rights reserved. Conduent and Conduent Agile Star are trademarks of Conduent Business Services, LLC in the United States and/or other countries. FYI® and For Your Information® are trademarks of Buck Consultants, LLC in the United States and/or other countries.