

GDPR and Pension Schemes: Lawful Basis for Processing Personal Data (Including Consent)

The processing of an individual’s personal data shall be lawful only if it meets one of six lawful bases. This basis (or bases relied upon) has to be explained in the privacy notice. Some rights are modified depending on the lawful basis for processing the personal data. For example, if consent is the lawful basis, individuals have a stronger right to have their data deleted.

This is the second in a series of six briefing notes about the General Data Protection Regulation (GDPR) that takes effect in the UK from 25 May 2018.

In this issue: [What are the lawful bases for processing personal data?](#) | [What does processing entail?](#) | [Conditions for Consent](#) | [Impact on Pension Schemes](#) | [Recommended Actions for Employers and Trustees](#) | [Further Reading](#) | [Types of Personal Data](#)

What are the lawful bases for processing personal data?

At least one of the following shall apply:

- The individual has given consent to the processing of his or her personal data for one or more specific purposes.
- Processing is necessary for the performance of a contract to which the individual is party or in order to take steps at the request of the data subject prior to entering into a contract.
- Processing is necessary for compliance with a legal obligation to which the controller is subject.
- Processing is necessary in order to protect the vital interests of the individual or of another natural person.
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
- Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party.

What does processing entail?

Definition

'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.

Conditions for Consent

Where this is the lawful basis for processing, the controller must be able to demonstrate that the individual has consented to processing of his or her personal data. This will usually be the lawful basis for special categories of personal data (see the table below).

However, consent will not always be the easiest or most appropriate lawful basis and there are alternatives, even for special categories of data.

A request for consent must be presented in a manner which is clearly distinguishable from other matters where the written declaration concerns other matters. It shall be in an intelligible and easily accessible form, using clear and plain language. It must specify why the data is needed and all the ways in which it might be used. A request can be made and consent given orally.

Consent can be withdrawn by the data subject at any time. This point must be made clear to the individual before they give consent and it shall be as easy to withdraw consent as to give it.

Impact on Pension Schemes

The Information Commissioner's Office (ICO) has issued [draft practical guidance](#) on how it interprets consent under the GDPR, giving its recommended approach to compliance and good practice. There is unlikely to be any guidance specifically relevant to pension schemes.

In its view, consent is only appropriate if the individual is being offered real choice and control over how their data is to be used. Also, if the data would still be processed without consent then asking for consent is misleading and inherently unfair. One of the requirements, where consent is used, is that consent can be withdrawn at any time. This may prove to be impractical for pension schemes.

The GDPR suggests that legitimate interest could exist where there is a relevant and appropriate relationship between the individual and the controller such as where the individual is a client or in the service of the controller. The ICO gives the example of an employer processing employee data and suggests that this is an example of where consent would not be the appropriate basis. Members join a pension scheme voluntarily in order to receive benefits and trustees and service providers need the members' personal data in order to administer the scheme correctly (paying the right benefits to the right beneficiaries at the right time).

Trustees need to comply with the provisions of the scheme documents and legislation (e.g. trust law, pensions and taxation law) in order to correctly fulfil the terms of their relationship with the members and may, therefore, have a legitimate interest in processing the members' personal data.

The Pensions Regulator also requires trustees to ensure they have accurate records of members' data. It is hoped that the Regulator will issue guidance on the specific issues for trustees and pension scheme administrators on the impact of the GDPR on these requirements.

Trustees may need to obtain explicit consent from members, particularly where they will be processing health data where a member applies to retire early due to ill health.

Another situation where explicit consent may be required is where trustees are considering to whom to pay discretionary death benefits. This will involve obtaining information about the personal relationships the deceased member had with potential beneficiaries at the time of death. This information may fall under the special categories of personal data and therefore trustees may need to ask for the consent of the potential beneficiaries when this information is collected. The pensions industry has asked the ICO for guidance on how to treat personal data used in consideration of death benefit cases.

Trustees (and particularly pension scheme administrators) usually hold on to personal data (of members and beneficiaries) for many years after members have transferred out of the pension scheme or where members have died. They may need to be able to prove that they no longer hold a liability for a member in the event of a claim in the future or prove that they exercised their discretion correctly. It is not clear whether this is a situation where the data being held for the purposes of the legitimate interests of trustees and/or pension scheme administrators would override the interests of the individual.

Recommended Actions for Employers and Trustees

- Determine the lawful basis for processing personal data in all circumstances, particularly ill health and 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.
- Audit what special categories of personal data are held by the trustees and by any service providers.
- Explain the lawful basis in privacy notices.
- Review any forms that contain requests for consent.
- Establish or review any procedures for obtaining consent as well as dealing with a member's request to withdraw their consent.

Further Reading

- Information Commissioner's Office (ICO): [Overview of the GDPR](#)
- FYI: [Preparing for the GDPR](#)
- FYI: [GDPR and Pension Schemes: Controllers and Processors](#)
- 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 |
|--|---|---|
| <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.