FYI®
For Your Information®
UK

Volume 2017 | Issue 64 | 1 September 2017

GDPR and Pension Schemes: Personal Data Breaches and Penalties

The General Data Protection Regulation (GDPR) requires controllers to report breaches (within 72 hours) where the individual is likely to suffer some form of damage (such as identity theft or a confidentiality breach) and notify the individual whose data has been breached (e.g. where it might leave them open to financial loss). Failure to report a breach to the Information Commissioner's Office when required could result in a fine, as well as a fine for the breach itself.

The maximum fines under the GDPR are 20 million euros for serious breaches (or 4% of annual worldwide turnover if higher) and 10 million euros for breaches of lesser provisions (or 2% of annual worldwide turnover if higher).

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

What is a personal data breach?

Definition
'Personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. It should be noted that it only covers actual breaches and not suspected breaches and is not limited to loss of data, but extends to unauthorised access.

Security of Processing

As expected, controllers and processors must take appropriate technical and organisational measures to protect their systems. They must also take the following actions (where appropriate):

- the pseudonymisation and encryption of personal data
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services

- the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

Breach Notification Process

The first step is for the controller to determine whether the personal data breach is likely to result in a risk to the rights and freedoms of individual living persons.

If this is the case, the controller must without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the Information Commissioner's Office (ICO). Where the notification is not made within 72 hours, it shall be accompanied by reasons for the delay.

Controllers must also document any personal data breaches, including the facts relating to the personal data breach, its effects and the remedial action taken. This will enable the ICO to verify compliance with the GDPR.

What details have to be included in the notification to the ICO?
Nature of the personal data breach including, where possible, the categories and approximate number of individuals concerned and the categories and approximate number of personal data records concerned.
Name and contact details of the data protection officer or other contact point where more information can be obtained.
Likely consequences of the personal data breach.
Measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

The next step is for the controller to determine whether the personal data breach is likely to result in a high risk to the rights and freedoms of individual living persons.

If this is the case, the controller must, without undue delay, communicate with the individual(s) affected, in clear and plain language, except where:

- the controller has implemented appropriate technical and organisational measures, such as those that render the data unintelligible to any person who is not authorised to access it, such as encryption
- the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of the affected individual is no longer likely to materialise
- it would involve disproportionate effort, in which case a public communication (or similar measure) can be made.

What details have to be included in the communication with affected individual(s)?
Nature of the personal data breach.
Name and contact details of the data protection officer or other contact point where more information can be obtained.
Likely consequences of the personal data breach.
Measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Processors have to advise controllers without undue delay after becoming aware of a personal data breach. They do not have to notify the ICO or affected individuals.

Penalties

Failure to report a breach when required under the GDPR could result in a fine, as well as a fine for the breach itself.

Breaches of certain provisions, for example, relating to the basic principles of processing, including conditions for consent, individuals' rights or transfers of personal data to a country outside the EEA, may result in fines of up to 20 million euros, or if higher, up to 4% of total worldwide annual turnover of the preceding financial year.

Other breaches, for example, failing to notify a personal data breach or put in place an adequate contract with a processor, fall into a lower tier and are subject to fines of up to 10 million euros, or if higher, up to 2% of total worldwide annual turnover of the preceding financial year.

Impact on Pension Schemes

Pension schemes will not be immune from security breaches.

Trustees (as data controllers) and possibly scheme actuaries (as joint data controllers) will be responsible for notifying personal data breaches to the ICO, unless the breach is unlikely to cause risk to individuals' rights and freedoms. They will also be responsible for doing so where the breach is caused by pension scheme administrators (the processors).

Whether the fines specifically referred to in the GDPR could apply to pension schemes (i.e. whether 'worldwide turnover' could be applied to a pension scheme's assets) is not clear. It would be for the ICO to apply penalties to trustees or to pension scheme administrators and these can be challenged by appeal to the courts.

Individuals have the right to bring a claim against a controller or a processor in court and can recover both material damage and non-material damage.

Recommended Actions for Employers and Trustees

- 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, to determine whether a breach would be notifiable.
- Review cyber-security measures, particularly for individual trustees (or directors of a corporate trustee).
- Establish a data breach policy, ensuring named individuals are familiar with the details and timescales.
- Ensure that contracts with service providers require notification to the trustees as soon as they are aware of a breach and details of how they can assist the trustees in enabling them to comply with the breach notification requirements.

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: 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: Rights of Individuals
- 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.

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.

CONDUENT