Data Protection

Brexit or no Brexit, pension scheme trustees, employers, administrators and third party providers must start to prepare for the new data protection regime which will apply next year.

Background

The EU General Data Protection Regulation (the "**GDPR**") replaces the current Data Protection Directive 95/46/EC (the "**Directive**") and its national implementing laws such as the UK Data Protection Act 1998. The GDPR will be effective in all members states from 25 May 2018.

Amongst the uncertainty created in the wake of Brexit, the implementation of the GDPR is one area where the Government's post Brexit agenda is clear; the Secretary of State in October 2016 confirmed that the GDPR will apply to the UK from 25 May 2018 and the ICO reiterated its commitment to "assisting businesses and public bodies to prepare to meet the requirements of the GDPR ahead of May 2018 and beyond". The ICO has produced an overview of the GDPR and supplemental guidance available on its website.

The GDPR will significantly change the data protection regime across the EU. Trustees, employers, actuaries, scheme administrators and third party providers will all be affected by the GDPR and may need to implement significant structural changes to comply with the new regime.

Given the prescriptive nature of the reforms and the significant penalties for non-compliance, preparation for compliance will need to begin in 2017.

Pensions context

Pension schemes – and actuaries to whom data is supplied for both consolidated exercises (e.g. valuations, insurance settlement or hedging projects) or individual exercises (e.g. transfers or (ill-health) early retirement quotes) are rich mines of personal, sensitive and financial data.

- **Data processing examples:** individual quotes; nomination of beneficiaries forms; online switches; liability management exercises; longevity hedges; buy-ins and buy-outs; the new "pensions dashboard" to aggregate data across schemes.
- **TPR:** "Trustees should undoubtedly be capturing GDPR and cyber security as a key risk on their risk registers".

Relevance of data protection law to actuaries

IFoA 2014 Guidance on Data Controller Responsibilities for Actuaries and Firms dealing with Personal Data (available on IFoA website) says:

- Scheme actuaries, as "Specialist Service Providers", are **data controllers** who must (i) individually register with the ICO and (ii) ensure compliance with the 8 data protection principles of the Data Protection Act 1998 (and in turn this will mean the GDPR).
- Scheme actuaries may be **joint data controllers** with their client (trustee) and/or firm.

Key issues for actuaries

- Identify which activities fall under your **personal appointment**, and which fall to your firm;
- **Allocate – and contractually document – responsibility** for (and liability protection in respect of) each data protection obligation as between (i) trustees and scheme actuary (engagement letters); and (ii) scheme actuary and their firm (employment contract/partnership agreement);
- Critically review this in the light of the GDPR's enhanced obligations and enforcement sanctions.

GDPR: In a nutshell

When?

It will apply in the UK (and all EU member states) from 25 May 2018.

What?

It governs how organisations can **collect, process, store** and **transfer** personal data.

Who?

It applies to the **processing of personal data** by:

a) data controllers and processors established in the EU; and

b) data controllers and processors outside the EU where their processing activities relate to the offering of goods or services (even for free) to data subjects within the EU OR to the monitoring of their behaviour.

The changes will affect pension scheme trustees, employers, actuaries, administrators and third party providers.

How?

In processing personal data, organisations must comply with the data protection principles under the GDPR.

For processing to be lawful under the GDPR, organisations must also identify a legal basis before the processing of personal data commences.

Sanctions

For serious breaches the potential maximum fine has increased to **€20 million or 4%** of the entire worldwide annual turnover in the preceding financial year.

For less serious infringements the potential maximum fine will be **€10 million or 2%** of entire worldwide annual turnover.

Kate.Atkinson@bakermckenzie.com (0207 919 1402)
Joanna.deFonseka@bakermckenzie.com (0207 919 1821)

GDPR – Action Plan for scheme trustees and scheme actuaries

	Overview	Consent	Rights of Data Subjects	Privacy Notices	Data Processor Obligations	Cross-border transfers	Notification of data breaches	Data Protection by Design and Default	Accountability
Requirement	The GDPR is applicable to the processing of personal data by controllers and processors established in the EU. This means that trustees, employers, actuaries, administrators and third party providers are all in scope. The supervisory authority in the UK is the ICO.	Where required, consent will be harder to obtain and rely on. Pension scheme members must be able to withdraw their consent. Consents must be clear, unambiguous, informed and transparent. Where consent is relied upon to legitimise the processing of sensitive data it must be explicit.	The range of existing rights for data subjects are preserved and extended. For example, the right to data portability, the right to erasure and the right to object to data profiling are new rights. This means significantly more information will need to be given to scheme members about the processing of their personal data. Infringements of the provisions relating to data subjects' rights are subject to the maximum level of fines.	The GDPR heralds a renewed emphasis on data subjects being given information in a "concise, transparent, intelligible and easily accessible form, using clear language" and an authoritative list of information that a privacy notice should contain.	Compliance obligations are directly imposed on processors, including implementing security measures, notifying data controllers of breaches and maintaining processing records. Processors will be directly liable for non-compliance. This change is significant for scheme administrators. Trustees, employers, scheme administrators, and actuaries must maintain a detailed record of processing activities which can be provided to the ICO on request.	The GDPR prohibits data transfers outside of the European Economic Area unless certain conditions are met. The cross-border transfer rules are retained and new requirements have been introduced, such as certification mechanisms and codes of conduct.	Any data breach must be reported to the ICO without undue delay (where feasible within 72 hours of becoming aware of a breach). In certain circumstances, data breaches will also need to be reported to scheme members.	Data protection by design and default are concepts which are codified into the GDPR. This means that members' privacy should be considered from the outset of each new process, product, service or application concerning a member's personal data. By default, only minimum amounts of personal data, as necessary for specific purposes, can be collected from members and processed.	The GDPR introduces prescriptive requirements for accountability. Trustees, employers, and scheme administrators – and where relevant actuaries - must not only comply with the GDPR's requirements but demonstrate how compliance has been achieved.
Action Plan	Carry out an information audit to find out what data you hold, where it comes from and who you share it with. Consider existing compliance (e.g. information about members' medical or physical health must be processed in compliance with the GDPR requirements) as well as future compliance. Review guidance released by the ICO and watch our for further guidance to be coming in the course of 2017/2018.	Identify existing processing activities legitimised through consent and determine whether they are GDPR compliant. Consent (including implied consent) obtained under the old data protection regime will be valid provided the GDPR's requirements are satisfied. Consider if an alternative legal basis can be relied upon (e.g. a legitimate interest of the data controller provided that it does not override the rights of the individuals) Ensure processes are in place to promptly honour any withdrawal of consent (within one month of a request).	Establish processes to identify and record any request from members and introduce measures to act on such requests promptly. Consider providing additional information to scheme members regarding the processing of their data.	As a priority, review existing privacy notices. Trustees and employers may need to update their existing notices to comply with the increased information mandated to be included by the GDPR.	Review existing data processing agreements and renegotiate where necessary. All data processing agreements will need to include new mandatory terms. Any new agreements should be written under the terms of the GDPR in 2017. Institute data mapping (which involves mapping all data flows) and other operational policies required to implement and maintain a detailed record of processing activity. Actuaries should work proactively with trustees, given their processor and data controller status.	Establish a comprehensive inventory of your cross-border data flows and design a strategy which will legitimise those transfers. Review/amend cross-border transfer strategy in light of GDPR requirements.	Review existing reporting structures and data incident management policies and procedures. Operational changes may be required to comply within this short window.	Introduce measures such a pseudonymisation or data minimisation designed to implement data protection principles from the outset of any decision concerning members' personal data.	Create and maintain a record of compliance. Review existing privacy approach. An internal governance structure may need to be implemented which fosters a culture of privacy from the top down.

Notes for actuaries:

- The GDPR imposes specific requirements on the relationship between joint controllers. These include that the agreement which allocates data protection responsibilities between an actuary and its firm or its trustee must (i) reflect the roles and responsibilities of each joint controller vis-à-vis data subjects; and (ii) the essence of the agreement shall be made available to data subjects. As such, we would expect the IFoA to reissue this key paragraph from 2014 Guidance: "*The ICO has provided a level of reassurance in terms of its enforcement policy relating to a processing activity that contravenes the DPA. Where the Scheme Actuary and his/her client and/or firm are joint data controllers, and there is a documented audit trail in place between the Scheme Actuary and his/her client and/or firm (as applicable) setting out which party is responsible for which elements of compliance with the DPA, the ICO would be likely to take into account how responsibility for compliance had been allocated. Therefore, if the contravention related to a processing activity allocated to the firm and/or the client, the ICO might not typically look to an individual Scheme Actuary in any enforcement action, except in the circumstances described in paragraph 6.2.7*."
- Ensure the contractual allocation of practical responsibility and legal risk remains appropriate in light of the GDPR. Be aware that, irrespective of the terms of the agreement between joint controllers, data subjects can exercise their GDPR rights in respect of each controller.
- Actuaries and their firms can expect greater engagement and challenge from trustees around data mapping, security, and accountability, i.e. knowing where data is at all times; enhanced security measures; and being able to demonstrate compliance – data audits are likely to increase.