HYMANS ROBERTSON

Sixty second summary

Pension Schemes & the General Data Protection Regulation

The European Union's General Data Protection Regulation will (despite Brexit) replace the UK's existing data protection legislation when it becomes applicable on 25 May 2018.[1] Its requirements are more onerous than current rules in many areas, including higher fines for serious breaches. As data controllers, the trustees or managers[2] of occupational pension schemes need to begin their preparations now.

Background

The trend towards globalization, technological developments, and the sheer scale of the data processing operations that have arisen since current data protection rules were introduced convinced the EU of the need for a stronger and more consistent data protection framework, backed by robust enforcement, that will provide more fairness and transparency for individuals. By contrast with the 1995 EU Directive that it replaces, member states do not need to pass domestic legislation to give effect to the new General Data Protection Regulation (GDPR).

Infringement penalties

The GDPR obliges national supervisory authorities—the Information Commissioner's Office (ICO), in the UK—to impose upon those who breach its requirements administrative fines that are '*effective, proportionate and dissuasive*'. The level of the fine in any particular instance will depend on considerations such as the nature and gravity of the infringement, and whether it was deliberate or negligent. The maximum fine for the least-serious infringements will be €10m or, where the transgressor is a business undertaking, two per cent of its annual turnover if that is higher. These limits are doubled for the most serious breaches. The maximum monetary penalty that the ICO can impose under current UK legislation is £0.5m.

New & enhanced rights for data subjects

The GDPR will provide data subjects—the members and beneficiaries of pension schemes—with enhanced rights of access to their personal data, and new rights of erasure (the 'right to be forgotten') and data portability.

As with current rules, trustees will need to identify the legal basis on which members' personal data are processed. Currently, this is often done by seeking members' consent to processing, especially when sensitive personal data (for example health information) is involved. The GDPR defines '*consent*' as '*any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing*', and emphasizes that it can no longer be inferred from silence, pre-ticked boxes or inactivity; consent is not freely given if data subjects are unable to refuse or withdraw it without suffering detriment. Other grounds for processing include, for example, when it is necessary for compliance with a legal obligation to which the data controller is subject, or in pursuit of the controller's legitimate interests. Regardless of the legal basis on which trustees decide to rely, members will have to be told how their data are used. The GDPR says that the necessary information must be provided '*in a concise, transparent, intelligible and easily accessible form, using clear and plain language*'.

[1] Regulation (EU) 2016/679.

[2] The GDPR applies to those responsible for public-service pension arrangements, such as the Local Government Pension Scheme (LGPS). For the remainder of this short summary, in the interests of brevity, references to trustees should be taken to include the managers of such schemes, in the absence of indications to the contrary.

Data processors and joint data controllers

The GDPR will, unlike the current rules, make data processors (those carrying out processing on the data controller's behalf) directly responsible for certain aspects of compliance. In the context of an occupational pension scheme, the typical data processor would be the providers of third-party administration and other services to the trustees. Where the trustees appoint professional advisers or a scheme actuary, they will as joint data controllers have to agree the allocation of responsibilities, and to communicate the essence of this arrangement to scheme members in an accessible format.

Accountability and record keeping

The trustees as data controllers need to be able to demonstrate how they comply with the GDPR. They and their appointed data processors will each have to maintain records of the processing activities for which they are responsible. They will be obliged to make those records available to the ICO on request.

Reporting breaches

Trustees will have to report data breaches to the ICO if there is a likelihood of risk to people's rights and freedoms. Such reports will have to be made '*without undue delay*' and where feasible within 72 hours of the trustees becoming aware of breaches (they can expect their processors to notify them of breaches without undue delay). If the breach is 'high risk' and is not mitigated by data encryption or other measures, the trustees will have to inform affected members without undue delay.

Data protection officers

In some circumstances (including where there is regular and systematic monitoring of individuals on a large scale), the GDPR will oblige the data controller (and the processor) to appoint a qualified person to fulfil the role of '*data protection officer*' (DPO), responsible for (amongst other things) advising the controller, monitoring compliance, and liaising with the ICO. Public authorities and bodies will be caught by this requirement; on the basis of the GDPR and the guidance that has been published so far, it seems at least arguable that the trustees of larger schemes will be too.[3] The DPO could be one of the trustees, or an external individual or consultancy firm.

Brexit

The GDPR will almost certainly become applicable before negotiations about the UK's exit from the EU have been concluded. Although the terms of the post-Brexit relationship between the UK and the EU will be decisive in many areas, the Government acknowledged in its 'Brexit' White Paper the need, in practice, for non-EU countries to have data protection standards equivalent to those of the EU, and said that it will '*seek to maintain the stability of data transfer between EU Member States and the UK.*'[4]

Trustees should be taking steps *now* to understand and document what data they have and how it is used. They should also become familiar with data subjects' rights under the GDPR, and when they will apply. In the pensions context, the new rules for processing by consent may prove extremely problematic, so trustees should consider whether another basis may apply: for example, that processing is necessary for the trustees' to pursue their legitimate interests (their duties under the scheme), or for compliance with a legal obligation to which they are subject.

Privacy notices (for example on forms or Web sites) will have to be reviewed and updated. Contractual arrangements with processors will have to be reviewed and updated, as the GDPR is more prescriptive about what needs to be set out in the agreement.

---

[3] Article 29 Data Protection Working Party, *Guidelines on Data Protection Officers* (WP 243 rev.01), <http://ec.europa.eu/newsroom/document.cfm?doc_id=44100>.

[4] *The United Kingdom's exit from and new partnership with the European Union* (Cm 9417), <www.gov.uk/government/uploads/system/uploads/attachment_data/file/589191/The_United_Kingdoms_exit_from_and_partnership_with_the_EU_Web.pdf>.