HYMANS ROBERTSON

Sixty second summary

Privacy Notices and the General Data Protection Regulation

One of the significant changes in UK data protection law arising from the new General Data Protection Regulation[1] is the need for greater transparency when processing personal data. Privacy notices will be an important tool in meeting the requirements.

Background

The General Data Protection Regulation (GDPR), which will comes into force on 25 May 2018, requires data controllers to provide clear and transparent information to individuals whose personal data is collected, in most cases at the time of collection of their data.

In relation to members of an occupational pension scheme, this responsibility falls most obviously upon the scheme trustees, who exercise overall control over the use of members' personal data. However, sponsoring employers may also have an interest in ensuring that individuals are informed about how their data is used if, for example, they commission advice or other services from advisers who need access to that personal data—when reviewing a funding strategy, perhaps. Moreover, the role that professional advisers play with respect to members' data may also need to be communicated.[2]

What needs to go into a privacy notice?

Privacy notices (also called fair-processing notices) under the GDPR are more detailed and specific than those hitherto required under the Data Protection Act 1998—although much of what is now mandatory has always been considered good practice in upholding the data protection principle of fairness. The minimum contents of the notice in a particular case will depend on whether the data is collected directly from the individual or obtained from another source. As well as contact details for the data controller and its data protection officer (if it has one), it must cover, amongst other things,

- the purposes of the processing and the legal basis on which it will proceed;
- any third parties to whom the data will be disclosed;
- data-retention policies;
- data subjects' rights, such as the ability to access their data and correct any mistakes, or to restrict, object to or withdraw consent for the processing; and
- information about any automatic decision-making.

Finally, where the data controller intends to further process the personal data for a purpose beyond that for which the data was collected, it must, prior to the new processing, provide the individual with information on that other purpose and with any relevant further information.

[1] Regulation (EU) 2016/679.
[2] For more information see our Sixty Second Summary, *Data protection: the "joint controller" issue* (September 2017).

Format of the privacy notice

Some discretion is permitted about the format in which the information is provided. The GDPR says it must be provided in a '*concise, transparent, intelligible and easily accessible form, using clear and plain language*'. It must be in writing, ordinarily, but that may be accomplished electronically—for example by email or on a website. The information may also be provided orally if the individual data subject asks for it in that form. Privacy information must be provided free of charge.

Timing of the privacy notice

Where personal data is being collected from individuals, privacy information must be provided at that point. Otherwise, privacy information must be provided within a reasonable period of having obtained the data (and within one month) and must be provided before any personal data is disclosed to a third party. So for new scheme members, a privacy notice could be provided in the welcome pack or other initial correspondence. For existing scheme members, summary funding statements, annual benefit statements or member newsletters all provide opportunities to communicate updated privacy information, either by including a copy of the privacy notice or pointing to where it can be found online.

Privacy notices need to be kept up-to-date and any significant changes should be communicated to individuals.

Infringement penalties

Failing to provide the mandatory privacy information is treated as one of the most serious infringements of the GDPR, liable to fines of up to €20,000,000 or for commercial undertakings, 4% of global turnover, whichever is higher.

Trustees and sponsoring employers should be taking steps now to understand and document what privacy information needs to be provided to scheme members. They may need to consult with their legal and other advisers (as well as each other). Privacy notices (including those appearing on forms or websites) should be reviewed and updated. Further guidance can be found on the ICO's website.[3]

Reviewing privacy notices is just one aspect of the preparations needed to ensure GDPR compliance. Please speak to your Hymans Robertson consultant if you would like an overview of the changes.

[3] *Privacy notices under the EU General Data Protection Regulation* <https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control/privacy-notices-under-the-eu-general-data-protection-regulation/>.