Ascot Lloyd
BENEFIT SOLUTIONS

0345 345 5111
info@ascotlloyd.co.uk
www.ascotlloyd.co.uk

Pensions briefing

August 2017

General Data Protection Regulation for trustees

UK data protection law will change from 25 May 2018 to make it fit for a digital era. The changes are driven by EU law but will go ahead in the UK whatever form Brexit takes.

General Data Protection Regulations

This provides a single EU legal framework for the processing of individuals' data. It recognises the technological advances of recent years and strengthens individuals' fundamental data protection rights. General Data Protection Regulation (GDPR) brings in a number of issues, which will affect pension schemes.

Data Protection Act - some aspects are retained

- The concepts of data controllers and data processors are still there but processors will become liable for their breaches of data protection legislation so that in many respects they will be treated in the same way as data controllers and be subject to the same compliance requirements.
- Personal data and sensitive personal data are also retained but the definitions have been widened.
- The eight data protection principles are also reflected, in strengthened form, in the GDPR.

Data controllers and processors – who is what?

- Pension trustees are data controllers whereas those who process the data on their behalf, e.g. the scheme administrators, are data processors.
- The scheme actuary is a data controller, while his firm is a data processor.
- The employer will be a data controller and may be a data processor.
- As the data controller, the trustees need to have written agreements with all their data processors.
- Both must have in place security measures to protect personal data against accidental or unlawful destruction, loss, alteration, disclosure or access.

Data audit – this will be required

This is an analysis of the nature of the data held and the way in which trustees and third parties hold and use the scheme's data. The audit could form the basis for the trustees' GDPR policy.

Member consent – a major and ongoing issue

In the past parties have deemed members' consent to holding data by including statements in booklets and other communications and allowing individuals to object to the data being held. This is known as 'implied consent' and is no longer sufficient. Where individual consent is required in future it must be positive 'affirmative consent'.

In addition the regulations require explicit consent for processing sensitive personal data but these data are not generally held for pension scheme purposes. Where consent is required, if data is used for multiple purposes, which is not defined, then multiple consents would be required.

If data is shared every third party must be named – so if administrators or actuaries are changed would that need to be communicated?

Consent can be withdrawn by a member at any time and must in any event be renewed every two years.

Legitimate interest – an alternative to individual member consent

In addition to individual consent, there are five alternative conditions that can enable the holding and processing of personal data. For pension schemes the most suitable is likely to be where that is necessary in

the pursuit of a legitimate interest by the data controller – viz. the operation of the pension scheme. The data audit will help establish what the data is and what it is used for, but if that alternative is used then the existing privacy notices in booklet and letters will need to be updated and made more explicit. Trustees will need to be guided by their legal advisers on whether this is a viable alternative in their scheme.

Contracts

Trustees will need to review contracts with data processors e.g. scheme administrators to ensure these are GDPR compliant and that the responsibilities are understood. This is likely to require the imposition of new terms detailing the more extensive obligations on the processors, who will counter with a request for additional indemnities from trustees.

Breaches

The time taken to notify the appropriate parties will be tightened and the fines are being increased.

Data protection officer

Private sector schemes will be free to appoint a data protection officer if they wish but will not be required to do so.

Data retention

Our June briefing on scheme administrator information obligations said that we should hold records for six years, following the year to which it relates. What is clear under GDPR is that data can only be held if there is a need to hold it. So if we acquire a new client then the previous data processor will need to destroy all of their records once relevant data has been passed on to us and there is no more scope for ongoing queries. In the past old records have been useful in answering historic member enquiries and guiding them as to whom to contact. For example, members often forget that they have transferred rights to an Insurance company – in the future, they will need to maintain their own records.

Our view

We are currently reviewing our existing procedures to ensure compliance, however the requirements are being constantly supplemented by the Information Commissioner's Office. In our case, we can relatively easily map how we use the data, but the audit will map where that comes from and who has access. At this point as administrators, the 'elephant in the room' is the need for affirmative member consent where trustees feel they cannot rely on the 'legitimate interest' principle. Where individual positive consents are required this can only add to current administration costs and the need for two-yearly renewal of that consent will cause uncertainty going forward over things like the present practice of contacting pensioners for certificates of existence – currently every three years – and the tracing of longer term deferred members in order to pay their benefits.

We will no doubt receive further clarifications before 25 May but there are clearly many questions still to be answered definitively. What is clear is that this is not the last time you will read about GDPR.