GDPR – Practical guidance for pension trustees

Love it or loath it; data protection legislation is here to stay and from 25 May 2018 is changing significantly.

We explore the changes to the law and suggest our '**Top 6 Actions for Pension Trustees**'.

The current legislation (Data Protection Act 1998 (**DPA**)) has been in place nearly 20 years and from next year will be replaced by the General Data Protection Regulations (GDPR). This is one matter which will not be shunted into the sidings with Brexit and full compliance will be required from day one.

So, with the starting gun fired what does this mean for pensions?

Let's start by looking at what the GDPR is?

The GDPR replaces the DPA. It applies to all EU member states and provides a single EU legal framework for the processing of individuals' data. In addition (and unlike the existing legislation), it now recognises the technological advances of recent years and strengthens individuals' fundamental data protection rights. In other words it is 'DPA plus'.

Is it all change from the DPA?

No, some aspects are retained. For example, there will still be the fundamental concepts of:-

- data controller and processor but note that, for the first time, data processors will be liable for breaches of data protection legislation so that in many respects they will be treated in the same way as data controllers and subject to the same compliance requirements.

- personal and sensitive personal data although in both cases the definitions have been widened; and

- processing in accordance with six data protection principles which look very similar to those under the DPA.

So far, so good. So what IS so different then?

Put very simply, quite a lot when you start to look at how it will operate on the ground. With pensions in mind, some significant changes are as follows.

1. Personal and sensitive personal data must be processed in accordance with certain set conditions. Yes, there are similar provisions under the DPA and so there is some overlap with the current data protection requirements. The devil is in the detail

though and when you start to drill down into each requirement you see that there are some significant differences.

2. The most pertinent change for pension schemes is probably that to do with the concept of consent. By way of reminder data processing may only occur after an appropriate legal basis for processing has been identified. The consent of the data subject to data processing is one such legal basis. Obtaining consent to processing personal and personal sensitive data will become much more difficult. Existing consent provisions may not be sufficient for GDPR purposes. It's also important to note that members have the right to withdraw consent at any time (part of the "right to be forgotten" provisions). This could have significant operational implications for pension schemes.

3. So, if trustees don't want to (or can't) rely on consent, is there another legal basis for data processing? Probably for pension schemes the obvious choice would be "the legitimate interests" basis, i.e. where data processing is necessary for the purposes of legitimate interests pursued by the data controller. However, in order to comply with this, members will need to be provided with detailed privacy notices. It's probably the case that most privacy notices at present will need to be updated to comply with the GDPR.

4. Trustees will need to review contracts with data processors (including scheme administrators) to ensure these are GDPR compliant. This is likely to require the imposition of new terms detailing the more extensive obligations. As a quid pro quo (and mindful of their own potential liability for breach of the GDPR), we expect data processors to seek additional indemnities from trustees.

5. And what if things do go wrong? The time frame for the notification of data breaches will become more onerous. Any breach will need to be notified to the Information Commission Officer without undue delay and where feasible within 72 hours of becoming aware of the breach.

   And if things go really wrong then for the most serious breaches the penalties are being increased up to 20 million euros (or for commercial entities the higher of 20 million euros or 4% of global turnover).

Top 6 actions for trustees

ACTION: PLAN

There is a lot to take in. The starting point is to recognise there is an issue and start to dedicate time and resources into getting the pension scheme GDPR ready for 25 May 2018.

ACTION: ASSESS

Assess the data protection risks to the pension scheme. This may require a data mapping exercise and a detailed understanding of how data processing and sharing works especially if there are any international data transfers.

ACTION: UPDATE

Update scheme governance processes and documentation to ensure compliance with the GDPR – in particular ensure that there is a suitable data breach protocol in place.

ACTION: REVIEW AND REPLACE

Review the current processing conditions for data processing and see if there are changes needed – in particular should trustees rely on consent or legitimate interests? The likely outcome is that a member communications exercise will be needed either to obtain GDPR compliant consents or put in place more detailed privacy notices.

ACTION: CHECK AND DECIDE

Check systems and policies to see how to respond to any member who wishes to have their data erased under the right to be forgotten and related rights.

ACTION: CHECK AND RENEGOTIATE

Review contracts between trustees and third parties – especially scheme administrators - to ensure they are GDPR compliant. As indicated above, data processors are likely to have increased liability for breaches under the GDPR and may seek greater indemnity protection from trustees.

Conclusion

Potentially the GDPR will have a significant impact on the way in which pension schemes are run. Although May 2018 may seem a long time away with compliance needed from day one, it is imperative that trustees and employers start to get their heads round how they will implement the new regime.

If you would like to discuss any aspect of this article further, please contact Rebecca Cooke or your usual contact in the pensions team on 0113 244 6100.

The information in this article is necessarily of a general nature. Specific advice should be sought for specific situations. If you have any queries or need any legal advice please feel free to contact Wrigleys Solicitors.