SQUIRE PATTON BOGGS

Pensions Trustees – Data Protection Gets Serious

July 2016

On 24 May 2016 a new General Data Protection Regulation (GDPR) was adopted by the European Union. It will have direct effect in all European Economic Area (EEA) countries, replacing the Data Protection Act 1998 from 25 May 2018. It will have a significant impact on pensions trustees, and the scale of the changes means that trustees need to start preparing now.

Why Will It Affect Trustees?

Trustees, or service providers on their behalf, process a great deal of personal data about pension plan members, pensioners and beneficiaries, some of it sensitive. Trustees are "data controllers" of this data, with responsibility for data protection compliance. Some of their service providers are their "data processors". Others, along with product providers, are co-data controllers with the trustees. Although the GDPR builds on the existing data protection legal structure, it extends obligations in a number of key areas. Importantly, penalties for non-compliance will increase by several orders of magnitude. For the most serious breaches, the penalties for trustees are up to €20 million and, for commercial entities, the higher of €20 million or 4% of global turnover. If more than one data controller or data processor is responsible for the breach, the Information Commissioner's Office (ICO) can choose to pursue whichever organisation has the deepest pockets. It would then be for that organisation to seek to obtain contributions from the other defaulters.

In addition, individuals will have the right to sue data controllers and/or processors, and not for profit consumer organisations can bring a form of "class action" on behalf of groups of individuals.

Key Changes Affecting Trustees

- **Data processors.** For the first time, data processors – service providers like pensions administrators and payroll processors – will have direct liability for breaches of the GDPR, and can be fined in the same way as data controllers. This is good news for trustees. However, this change in processors' risk profiles is likely to mean that they will push for indemnities from trustees. Trustees will continue to have the obligation to make upfront and ongoing checks into the security measures their processors will apply, and it will be mandatory to include much more extensive obligations in processor agreements than are compulsory at present.
- **Privacy notices and consent.** Much more emphasis is being placed on ensuring that individuals are given clear information as to what is done with their data, by means of privacy or fair processing notices. In addition, where the consent of an individual is needed, it must be spelled out in very plain language exactly what the individual is consenting to, as well as the fact that they can withdraw their consent at any time. Trustees will need to revisit both their privacy policies and any consent documentation.
- **Records of data processed.** For the first time, it will be mandatory for controllers and processors to keep full records of exactly what personal data is processed, for what purposes, how and by whom, and with whom it is shared, as well as the security measures applied to it and how long it is to be kept.
- **Data breach reporting.** It will become mandatory to notify the Information Commissioner about data breaches that cause a risk to the individuals whose data is compromised. This must be done within 72 hours of learning about the breach. This makes it critical that trustees have a robust data breach response plan, so that they are able to respond within the necessary timeframes to a data breach.
- **Transfers outside the EEA.** Many service providers now provide at least some back office services from outside the EEA (i.e. the countries of the European Union plus Norway, Iceland and Liechtenstein). It will become critically important that, where this happens, protections have been put in place to ensure that the data will be adequately protected. Currently, the only relatively cheap and practicable option is to ensure that the relevant companies sign up to Standard Contractual Clauses (sometimes called Model Clauses) approved by the European Commission.
- **Privacy Impact Assessments.** These will become mandatory if the trustees ever undertake high risk processing.
- **Data protection by design and by default.** The GDPR places greater emphasis on data controllers ensuring that data protection will be complied with by designing systems and processes that minimise the data collected, and ensuring that data protection compliance is built into the system/process.

What Effect Will Brexit Have?

As the GDPR comes into force on 25 May 2018, and the negotiations around Brexit are likely to take at least two years from the date the government serves a notice on the EU of its intention to leave, the GDPR will come into force in the UK. The position after Brexit will depend partly on the terms of Britain's access to the EU internal market going forward. If the UK follows the Norwegian or Swiss model, it will have to agree to comply with the GDPR in full. Even if the UK opts for a looser relationship with the EU, in order to safeguard the free flow of data between the UK and Europe, the UK will need to agree to comply with provisions equivalent to the GDPR. The ICO has already stated that it will be making this case to the government. Trustees will, therefore, need to start addressing compliance with the GDPR now. If they do not, they are likely to find that they will not be in a position to comply when the GDPR or its equivalent comes into force.

What Do Trustees Need to Do Now?

- **Negotiating contracts with service providers**
  - **New contracts.** Trustees currently negotiating contracts with service or product providers that will or may continue beyond May 2018 will need to incorporate the new mandatory provisions required to be incorporated in agreements with processors. They will also need to ensure that limitation of liability provisions incorporate the maximum protections available to trustees.

    This will be particularly important for trustees negotiating administration services agreements. It would be logical to require plan administrators to keep the mandatory records about the personal data processed in relation to the plan. If this is not incorporated in contracts at the outset, administrators are more likely to resist providing this service, and/or to charge additionally for it.

    In addition to administration contracts, this may also be relevant for other contracts where personal data is passed on – such as buy-in contracts with insurance providers, or where third party consultants and/or financial advisors are appointed for liability management exercises.

    Even where the product provider or service provider is a data controller, the trustees will need to consider whether they wish to incorporate specific provisions allocating responsibility and liability for breaches of the GDPR as between the contracting parties.
  - **Existing contracts.** It would also be advisable for trustees to review their existing contracts with data processor service providers. Many do not contain the provisions that are mandatory under current law, meaning that, if the processor caused the breach, it would be the trustees that would be held responsible and, potentially, fined. Trustees can, at the same time, negotiate for the inclusion of the provisions that will be mandatory under the GDPR.

    It will also become all the more important that the trustees undertake upfront and ongoing checks into the security measures their processors will adopt. We can assist by providing a questionnaire that enables trustees to undertake these checks and also evidence that they have done so.

    Wherever personal data may be transferred to or accessed from outside the EEA, the contracts will need to incorporate Standard Contractual Clauses or another means of ensuring adequacy of protection.
- **Privacy notices and consent.** Many trustees currently only provide limited privacy notices to their members. Trustees will need to review their privacy notices and revise them to include all the information that will be mandatory. As consent to processing can be withdrawn at any time, trustees may wish to minimise, as far as they legally can, the use of consent as a justification for the processing. Where consent is needed, they will need to ensure that it is separately set out in plain language so that there can be no doubt that the relevant individual is giving fully informed consent.
- **Records of data processed.** When the data mapping required under the GDPR is undertaken by the trustees, or by administrators on their behalf, this will also assist the trustees in identifying, and remedying, any gaps in their data protection compliance.
- **Data breach response plan.** It is essential that trustees put in place a robust data breach response plan. The 72 hour notification requirement is very short. Often, such breaches occur on a Friday evening or over the weekend, or as a business closes down for the holidays. Having a data breach response plan setting out the contact details (including out of hours contact information) of all the internal and external people who will need to be involved, along with details of what actions will need to be taken in the event of a data breach can mean the difference between a manageable problem and a financial, regulatory and PR disaster.

Next Steps

The actions above are the most urgent for trustees. Others, like the carrying out of privacy impact assessments, can be undertaken once guidance on the circumstances in which they will be mandatory has been provided by the national regulators.

Further Information

We are already assisting clients in taking all of the actions mentioned above. If you need help in any of these areas, please contact any of the pensions partners listed or your usual contact in the pensions team, or one of our team of data protection experts with specific experience in advising pensions trustees (Caroline Egan, Francesca Fellowes or Stuart James).

Catherine McKenna
Partner, Leeds
T +44 113 284 7045
E catherine.mckenna@squirepb.com

Anthea Whitton
Partner, Leeds
T +44 113 284 7364
E anthea.whitton@squirepb.com

David Griffiths
Partner, Manchester
T +44 161 830 5359
E david.griffiths@squirepb.com

Wendy Hunter
Partner, London
T +44 207 655 1119
E wendy.hunter@squirepb.com

Matthew Giles
Partner, Birmingham
T +44 121 222 3296
E matthew.giles@squirepb.com

@SPB_Global