EU Data Protection reform

Six top tips for pension scheme trustees

After more than four years of negotiations, the new EU data protection framework has finally been agreed. Following a two-year transition period, the General Data Protection Regulation (GDPR) will apply in all member states from 25 May 2018.

The GDPR will completely overhaul the current data protection laws in the UK as well as Europe. It has a greater emphasis on formal compliance processes and imposes substantial new obligations on trustees in the collection and use of personal data. Trustees should therefore use the current 24-month transition period to fully review their existing processes and introduce new policies and procedures to prepare for the GDPR.

Terminology in a pensions context

As with any specialist area of law there is some basic terminology to understand. Helpfully this has not changed from the current terminology:

- A "data controller" is a person or body, which determines the purposes and means of processing personal data. In the pension scheme context, in the majority of cases the pension scheme trustee will be the data controller.
- A "data processor" is a third party who process the data on the data controller's behalf. Data processors will include administrators, advisers and annuity providers.

We have set out below six key areas of the GDPR which will have a significant impact on pension trustees:

1 Member consent

Obtaining valid consent from a member will be much harder under the GDPR. Member consent to data processing will need to be "freely given, specific, informed and unambiguous". Consent will need to consist of a positive action, it cannot be inferred from silence, pre-ticked boxes or inactivity.

As trustees usually obtain consent from members to process their data as part of the "on-boarding" process of the scheme, such consent will need to be reviewed to ensure that it is compliant with the GDPR requirements. This will require more detailed information about the data processing to be provided for valid consent and that the consent is clearly distinguishable and in an intelligible and easily accessible form. There will also be duties to inform members of, for example:

- the period for which the personal data will be stored;
- the different rights available to them; and
- whether the trustee will transfer their data internationally.

Trustees should review their procedures to obtain and record consent to check if they are in line with the new GDPR requirements.

2 Use of data processors

Under current law, only data controllers are legally responsible for complying with data protection requirements. Under the GDPR, data processors will be liable independently (and with data controllers) for damages caused by their processing activities.

This is a significant change and is likely to lead to the renegotiation of service provider agreements. This may involve longer contractual negotiations as the liability position between the parties is agreed.

3 Enhanced data protection rights for members

The GDPR aims to give data subjects more control of their personal data. It enshrines a wide range of existing and new rights for individuals in respect of their personal data. These include:

- the right to access data;
- the right to erasure (e.g. right to be forgotten);
- the right to data portability (i.e. to transfer your personal data to a new service provider); and
- the right to object to certain processing activities and also to decisions taken by automated processes.

Trustees should ensure that they have processes in place to respond quickly and consistently to members who assert these enhanced rights.

4 Onerous penalties

The GDPR also introduces significantly higher penalties for breaching data protection requirements. Currently, the maximum fine which can be imposed for breaching UK data protection law is £500,000. Breaching GDPR can lead to fines of up to €20 million (or 4% global turnover where relevant).

As a result of this increase, it is important that trustees are fully aware of their obligations under GDPR and implement processes to address and mitigate the risk of breaches. Trustees should also update risk registers and review insurance arrangements currently in place.

5 Data breaches

Under the GDPR, trustees must notify a security breach to the supervisory authority "without undue delay" and within 72 hours of becoming aware of it. In certain "high risk" circumstances, the trustees may also need to notify the data subjects (e.g. members) of the data breach. It is therefore important that trustees review their breach management policies to ensure adequate procedures are in place for handling data breaches, especially ensuring that appropriate notification can be made within the timescales.

6 Data protection officer

Organisations will be required to appoint a data protection officer (DPO) if they are handling a significant amount of sensitive data or monitoring the behaviour of individuals.

Given the nature of pension trustees' responsibilities and the fact that they are collecting and processing health data (for example, for actuarial valuations or ill-health decisions), trustees may be required to appoint a DPO. We recommend that trustees consider appointing a DPO, even if not strictly required.

The DPO is a specialist role and initially we expect there to be a capacity crunch as staff and contractors train up into this role. Trustees need to consider carefully the duties and responsibilities of the DPO and the skills and experience necessary. Dentons is able to help with this.

Trustees appointing a DPO should do so in the near future, in any event well in advance of 25 May 2018.

Next steps

Now is the time to start planning for compliance with the GDPR. Dentons can provide a bespoke GDPR readiness plan and roadmap. In addition, we recommend that a GDPR compliance gap analysis is performed to identify the areas of material non-compliance and take action to address these.

© 2016 Dentons.

Dentons is a global legal practice providing client services worldwide through its member firms and affiliates. This publication is not designed to provide legal or other advice and you should not take, or refrain from taking, action based on its content. Attorney Advertising.

Dentons UKMEA LLP is a limited liability partnership registered in England and Wales under no. OC322045. It is authorised and regulated by the Solicitors Regulation Authority. A list of its members is open for inspection at its registered office: One Fleet Place, London EC4M 7WS. Any reference to a "partner" means a person who is a partner, member, consultant or employee with equivalent standing and qualifications in one of Dentons' affiliates. Please see dentons.com for Legal Notices.

29503-EU Data protection reform – 16/06/2016