Pensions Update - Special Edition

April 2016

BAKER & McKENZIE

It expected that the General Data Protection Regulation (the "GDPR") will be introduced in late Spring 2016. Once formally adopted, this piece of legislation will significantly change the data protection regime across the whole of the EU. Trustees, employers and scheme administrators will all have to take steps now to ensure that their data processing activities are compliant with the new regime, which will become law in the UK in 2018.

What is the current position?

The Data Protection Act 1998 implements the current EU data protection requirements in the UK. Trustees, employers and administrators have to ensure that their data processing activities comply with its requirements.

How will the GDPR change the current position?

The GDPR is directly applicable to Member States. This means that Member States have to implement its requirements without passing any implementing legislation. The intention is to harmonise the data protection regime across the EU by replacing the old patchwork of different rules with a single data protection regime. This means that an entirely new framework for data protection is coming into force and steps will need to be taken in order to comply.

What are the key changes and how should you respond?

The key changes that will be most relevant to those involved with the administration of pension schemes are likely to be:

- The territorial scope of the GDPR is wide. Non-EU organisations will have to comply with it where they are involved in monitoring EU data subjects' behaviour. This may be of concern to employers (or scheme administrators) where group companies located outside the EU handle members' data. Such companies will have to ensure that they comply with the GDPR in addition to any data protection laws applicable in the territories in which they operate.

- At present, in the UK, the maximum fine for breaching data protection requirements is £500,000. This will significantly increase under the GDPR, to the greater of 20 million euros or 4% of annual worldwide turnover for significant breaches, and the greater of 10 millions euros or 2% of annual worldwide turnover for breaches of lesser provisions.

- Extensive responsibilities will be placed directly on data processors. This change is likely to be of particular concern to administrators. They will have to ensure that their data protection policies and procedures comply with the new requirements. In addition, trustees and employers should check their contracts with their administrators and other data processors to ensure that they reflect the new requirements and to determine which party will bear any additional costs that might be incurred due to the changes in the law.

- It is likely to be harder under the GDPR to satisfy the requirements for obtaining consent to data processing. Consent must be freely given, specific, informed and unambiguous; either by statement or clear affirmative action. Explicit consent must be given for the processing of sensitive data. If the request for consent is made in writing that request must be made in clear and plain language. Moreover, trustees and employers should provide members (data subjects) with the ability to withdraw consent at any time. Trustees and employers should, therefore, review the language used in any documents in which members' consent to data processing has been sought. If the language

This newsletter is for information purposes only. Its contents do not constitute legal advice and should not be regarded as a substitute for detailed advice in individual cases.

If you wish to discuss any of these issues further, please contact your usual Baker & McKenzie lawyer.

Jeanette Holland
jeanette.holland@bakermckenzie.com

Robert West
robert.west@bakermckenzie.com

Arron Slocombe
arron.slocombe@bakermckenzie.com

Chantal Thompson
chantal.thompson@bakermckenzie.com

is inadequate to satisfy the new requirements, further member consent could be required.

- Individuals will have the right to request that their personal data be deleted in certain circumstances (commonly known as the "right to be forgotten"). Furthermore, individuals will gain the right to object to certain types of data processing. Trustees and employers should consider the policies and procedures that they may have to put in place to deal with any such requests and objections from members.

- The GDPR will require both data controllers and data processors to maintain internal records of the data processing activities they carry out. Data controllers will also have to conduct a data protection impact assessment for riskier processing activities and will have to implement data protection measures "by design and by default". Trustees and employers should be aware of the additional administrative burden that these new requirements are likely place on them. As a first step, they should review their existing policies and procedures to determine the changes that will have to be made.

- Data controllers will be required to notify data breaches to supervisory authorities without undue delay and, where feasible, no later than 72 hours of becoming aware of the breach. Data controllers will also be required to notify individuals of the breach if it is likely to pose a "high risk" to their rights and freedoms. Trustees and employers will have to ensure that they have appropriate procedures in place to respond to data breaches and to make any notifications within the required timescales.

When is this happening?

As the final text was agreed by the European Commission, the Parliament and the Council in December last year, it is likely that the GDPR will soon be formally adopted. The new requirements described above are expected to come into force in 2018. However, the extent of the changes to the current data protection regime mean that trustees, employers and administrators should already be thinking about how to modify their systems and processes to ensure their compliance with the GDPR.

What should you do next?

We expect that all organisations will have to make changes to their data protection policies, procedures and contracts. As there will be substantial penalties for breach of the new requirements, we would recommend that you seek advice to ensure that you are able to start thinking about any changes that might be required well in advance of the GDPR's coming into force.

We will be hosting a Breakfast Briefing on 27 April where we will be joined by Dyann Heward-Mills, Data Protection Partner, to discuss this topic in further detail. In the meantime, please do get in touch with your Baker & McKenzie LLP contact if you would like to discuss this further.

> Back to Top

Baker & McKenzie International is a Swiss Verein with member law firms around the world. In accordance with the common terminology used in professional service organizations, reference to a "partner" means a person who is a partner, or equivalent, in such a law firm. Similarly, reference to an "office" means an office of any such law firm.

Before you send an e-mail to Baker & McKenzie, please be aware that your communications with us through this message will not create a lawyer-client relationship with us. Do not send us any information that you or anyone else considers to be confidential or secret unless we have first agreed to be your lawyers in that matter. Any information you send us before we agree to be your lawyers cannot be protected from disclosure.

If you wish to opt out of these communications, please click here