BROADSTONE

PENSION SCHEMES AND THE GENERAL DATA PROTECTION REGULATIONS (GDPR) AND CYBER SECURITY

From 25 May 2018 the European Union's General Data Protection Regulation (GDPR) will come into force in all EU member states including (despite Brexit) the UK.

This will replace the UK's existing Data Protection legislation and its requirements are more onerous than the current legislation, including higher fines for serious breaches.

BACKGROUND

With the rise of technological innovation the last two decades have seen an explosion in the volume of data being used since the last Data Protection legislation was drafted. The EU wish to implement a stronger framework, backed by rigorous enforcement, to offer a higher level of protection for individuals.

The GDPR, while building on the foundations of the Data Protection Act 1998, nevertheless introduces a number of new requirements and trustees, employers (and us as your advisers) will need to consider the following areas to prepare for GDPR:

- Potential penalties on infringement
- Enhanced rights for data subjects
- Obligations of data controllers and joint data controllers
- The role of the Data Protection Officer
- Demonstrating compliance with the GDPR

POTENTIAL PENALTIES FOR INFRINGEMENTS

Given the large increase in potential penalties this is the area of the GDPR that has received most attention to date. From a maximum of £500,000 under existing Data Protection legislation the penalties can potentially grow to the higher of 20 million euros or 4% of annual turnover if higher. The figures will appear eye watering but the GDPR obliges the ICO to administer fines that are *'effective, proportionate and dissuasive'.*

It remains to be seen how the penalties will be applied in practice but the scale will certainly focus the minds of many organisation in the run up to its introduction.

ENHANCED RIGHTS FOR DATA SUBJECTS

The changes will enhance the rights of data subjects (pension scheme members and beneficiaries) to access their personal data and introduce new rights surrounding the 'right to be forgotten'.

Trustees will **need to identify the legal basis on which personal data is processed**, typically through member consent. However, the GDPR tightens up the basis under which consent can be obtained and removes the ability to rely on silence or inactivity or the use of pre-ticked boxes. Instead consent must be a *'freely given, specific, informed and unambiguous indication of the data subjects wishes'* with *'...clear affirmative action signifies agreement to the processing'.* **Members will also have to be told how their data is used** *'....using clear and plain language.' 'Explicit consent'* for sensitive personal data will also need to be given.

Trustees will need to **consider taking advice on the legal basis underpinning their use of data and following that consider an update to their privacy notices**. We also recommend **adding the GDPR to the Trustee Risk Register** to ensure it receives the appropriate level of focus ahead of May 2018.

OBLIGATIONS OF DATA PROCESSORS AND JOINT DATA CONTROLLERS

The GDPR will increase the level of responsibility for data processors (for example your pension administrator) making them directly responsible for elements of compliance with the GDPR. The Scheme Actuary is typically joint data controller with the trustees and you will need to agree the allocation of responsibilities and provide details of the agreed split to scheme members.

Broadstone is currently undertaking a review of its terms of business to reflect the required changes which will be communicated to you in advance of the changes. We will seek to agree an appropriate split of responsibilities and document this accordingly. Trustees will also potentially **need to review existing terms with other providers**.

THE ROLE OF THE DATA PROTECTION OFFICER

The GDPR may oblige organisations to appoint a person to fulfil the role of Data Protection Officer who will be responsible for monitoring compliance with the GDPR (Broadstone already has a nominated Data Protection Officer). There is some debate as to whether pension schemes, particularly larger arrangements, may also need to appoint Data Protection Officers.

This is an area of some conjecture and Broadstone recommends trustees **keep a watching brief over the coming months to understand if there is any scope to be impacted by this requirement.** Clarification is likely to be driven by some of the larger UK pension arrangements who are most at risk of being affected.

DEMONSTRATING COMPLIANCE WITH THE GDPR

Both trustees and the Scheme Actuary as Data Controllers need to evidence their compliance with the GDPR (together with their appointed Data Processors). In the event of a breach reports to the Information Commissioners Office (ICO) will need to be made within 72 hours. If the breach is 'high risk' trustees will also need to inform members *'without undue delay'*.

Broadstone has formed a GDPR Steering Committee to co-ordinate the activities required internally to meet those requirements and we will use the resources of this group to engage with you and help you as far as possible. It is also likely trustees **may seek independent advice on their obligations under the GDPR, particularly given the current level of ambiguity on some elements**.

CYBER SECURITY

The issue of Cyber Security clearly has the potential to impact on the requirements of the GDPR and the recent experience within the NHS and other organisations highlights the threat of Cyber Security.

Within Broadstone we are confident we have robust defences against cyber-attack and our systems are regularly tested. To provide some reassurance we are currently undergoing an external assessment of our Cyber Security defences and are aiming to achieve the Government supported Cyber Essentials Plus accreditation. This will provide external accreditation of the adequacy of our existing defences against cyber-attack. We expect to complete the process in the autumn and we will confirm our accreditation to you in due course.

SUMMARY

The GDPR builds on the existing Data Protection framework but will introduce changes to the way we need to work collectively with you to ensure pension scheme data is secure and the rights of privacy for pension scheme members is respected. We will continue to engage with you over the coming months to ensure we are fully prepared ahead of the changes being introduced on 25 May 2018.

CONTACT US TODAY

Paul Noone
Director, Trustee Services
55 Baker Street
London
W1U 8EW

+44 020 3869 6836
paul.noone@broadstone.co.uk

For more information on our wider pension and employee benefit services contact:

www.broadstone.co.uk
corporate@broadstone.co.uk

55 Baker Street
London
W1U 8EW
United Kingdom

BROADSTONE

TS/GDPR JUNE 2017