PENSIONS AND LIFETIME SAVINGS ASSOCIATION

GDPR – TOP TEN ACTIONS FOR PENSION SCHEMES

The General Data Protection Regulation (GDPR) will take effect from 25 May 2018. This is a major reform that will affect all organisations that hold personal data, and pension schemes are no exception. As it is an EU regulation it will not need to be transposed into UK law in order to take effect. Nevertheless, to ensure legal continuity post-Brexit its provisions will be implemented via a new Data Protection Act. A statement of intent regarding this bill was published on 7 August. Trustees and other senior decision-makers will wish to take action on this important issue.

While GDPR builds on the principles established by the 1998 Data Protection Act, there are some actions that you will need to take before it is implemented. This document is intended to provide an introduction to GDPR and is not a replacement for professional advice.

1 START PLANNING EARLY – IT'S A JOURNEY AND YOU'LL NEED A MAP

GDPR compliance is not something that can be achieved overnight. Depending on the complexity of your scheme there could be significant lead-in times for IT development or training. You may need to devote significant resources to your project in order to ensure compliance. This means that you need to start informing key decision makers and operational managers now. It is also essential that Trustees and senior decision makers have a strong level of understanding themselves.

You will only know the scale of the challenge when you have mapped out all of the places where data is gathered, held and processed.

2 DO YOU NEED WHAT YOU HAVE? – JUST BECAUSE YOU HAVE THE DATA DOESN'T MEAN YOU NEED IT

GDPR will require you to analyse the data you hold and consider whether you have the right to hold it, this also applies to data that is held on your behalf. You should only be holding personal data when there is a legitimate reason. If you fail to delete data that you no longer have a legal basis for holding, you could be in breach of the regulation. A thorough analysis of the data you hold is an essential part of becoming compliant.

3 REVISING THE SMALL PRINT – THE DEVIL IS IN THE DETAIL

GDPR is adding to the Data Protection Act requirement to give consumers certain specified pieces of information relating to privacy and their rights. Data subjects must be notified of the legal basis for processing their data and given details about the rights they have. You will need to examine the privacy notices that you distribute and ensure that they are GDPR-compliant.

You will also need to work with administrators and all other contractors to ensure that the clauses within your contracts and service level agreements are GDPR-compliant. These contracts will almost certainly have to be revised, so you should allow sufficient time to enable this to happen.

4 SYSTEMS AND PROCESSES – COMPLIANCE BY DESIGN

One of the ways in which you can demonstrate compliance with GDPR is through the systems and processes that your scheme has. This is phrased as 'compliance by the design' in the regulation and it is something that you should start planning for.

GDPR will also require Data Protection Impact assessments to be carried out in certain circumstances. For example, when you process large and unique categories of data, or when implementing new technology, it will be a legal requirement to carry out a risk assessment.

5 CONSUMER RIGHTS – IT'S THEIR DATA

GDPR reaffirms and reinforces the rights that were first established under the Data Protection Act and introduces others. GDPR gives individuals the following rights:

- the right to be informed;
- the right to access;
- the right to rectification;
- the right to erasure where appropriate;
- the right to restrict processing;
- the right to data portability;
- the right to object;
- the right not to be subject to automated decision-making.

You will need to examine how your scheme will ensure compliance with these rights. You should pay particular attention to amendments to the right to access, which shorten the amount of time for a response to a data subject access request to one month.

6 WHEN CAN I PROCESS – WHAT IS YOUR LEGAL BASIS?

The Information Commissioners Office (ICO) has confirmed that the legal bases that were applicable under the Data Protection Act will remain. Schemes may wish to rely on 'legitimate interest' or 'performance of a legal obligation' in most contexts. There are, however, some important changes to the ways in which consent is obtained and you will need to examine them and record your reasoning if you wish to depend on it as a lawful basis.

7 PERSONAL OR SENSITIVE? – MANAGING THE DISTINCTION

There are some significant additions to the definition of sensitive personal data that could present a challenge for your schemes. The inclusion of sexual orientation as personal data could mean that the name of one of your data subject's spouses could be deemed sensitive personal information. You will be under greater restrictions when processing this kind of data.

Additionally the inclusion of genetic and biometric data could present a challenge if your scheme processes medical data. This is an area that you should examine in great detail to ensure that the correct procedures are used when processing information.

8 BREACHES AND FINES – A BRAVE NEW WORLD

One of the biggest changes that the implementation of GDPR will introduce is in the potential scale of the fines that businesses can be subject to. This has increased from £500,000 to £17,000,000 (or 4% of global turnover). This new system of sanctions is proportionate to the increase in the amount of data held by private companies since 1998 and the potential harm that can be caused by breaches. Provisions within GDPR also mean that compensatory awards for the upset or distress caused to data subjects by a breach can now be made.

In addition to the new financial penalties, there will be a new requirement to report breaches to the Information Commissioner without 'undue delay' and no later 72 hours after discovery. If a breach is likely to impact on the rights or freedoms of an individual then you will have to notify the individual as well as the ICO.

9 ROLE OF THE DPO – GREATER RESPONSIBLITIES

Under the Data Protection Act 1998 there was no specific requirement to appoint a Data Protection Officer (DPO). Under GDPR organisations must appoint one if local laws require it (this will become clear when the new Data Protection Bill is published) or when the organisation's activities involve:

- regular and systematic monitoring of data; or
- processing Sensitive Personal Data on a large scale.

This might mean that you will have to appoint a DPO. If you do, you will also have to ensure that your DPO is suitably trained and is senior enough within the organisation to be able to perform their role without being subject to undue pressure. Start thinking about whether you need a DPO and, if so, who your DPO could be and what training they will need.

10 DATA PROCESSED OVERSEAS – TIGHTENING THE PERIMETER

One area that could require significant change is the strengthening of regulation around cross-border data transfers. Like the Data Protection Act, GDPR forbids this apart from in certain circumstances. Under GDPR some jurisdictions will be considered 'adequate' and will be placed on a white list; this list will be controlled by the European Commission and will take into account issues such as fundamental freedoms and the ability of the receiving jurisdiction to seize the data. As the UK will be leaving the European Union, the impact of such a regime is unclear. If you know of a subsidiary or administrator that engages in this kind of activity then action could be required.

Pensions and Lifetime Savings Association
Cheapside House, 138 Cheapside, London EC2V 6AE
T: 020 7601 1700 E: plsa@plsa.co.uk **www.plsa.co.uk**