The Great Data Protection Revolution

Personal data ('data') is central to the operation of pension arrangements. Schemes, providers and third-party administrators have to hold huge amounts of data on members to enable the arrangement to operate successfully and it is vital that this data is held securely and only processed in accordance with legislative requirements.

Currently, the framework for data protection is provided for by the Data Protection Act 1998 '(DPA '98'), however a new, far more stringent, regime is on its way.

The General Data Protection Regulation ('GDPR') is a new European Regulation that will directly apply to all organisations (regardless of location) processing the personal data of individuals residing in the European Union from 25 May 2018, without any need for it to be enshrined in UK legislation.

Despite Brexit, it would be wrong to assume that, as the changes are being introduced under European Regulations, we can simply turn a blind eye to them. The UK Government has already published a new Data Protection Bill that will effectively enshrine the main provisions of the GDPR directly into UK legislation. All pension schemes and providers will, therefore, need to comply with the new requirements.

The GDPR is not just a minor tinkering with the existing provisions. According to the Information Commissioner, it is "*the biggest change to data protection law for a generation*". As another commentator put it, under the GDPR, you need to "*think of data as asbestos: keep it to an absolute minimum, manage it very carefully and dispose of it as soon as possible*".
This does, of course, pose particular challenges for pension schemes and providers, given the huge amounts of data that schemes tend to accumulate and the long period of time for which it needs to be held.

Although the GDPR reflects many of the principles that underpin the DPA '98, it would be extremely unwise for any organisation that is fully compliant with the DPA '98 to assume that they are 'GDPR ready'. All organisations that process individuals' data will have to review and update their processes and procedures to ensure that they are - and can demonstrate that they are – complying with the GDPR and that data protection is an integral part of any data processing activity, rather than just an afterthought.

In this Aries Insight we look at the key differences between the DPA '98 and the GDPR and highlight some of the actions that may be necessary to prepare for the arrival of the GDPR. We will also identify additional sources of information that are available to help in this planning.

Overview of the GDPR

The GDPR builds on and expands the principles in the DPA '98. It: increases individuals' rights; imposes new duties on data processors; introduces new requirements for reporting breaches of the Regulations; and hugely increases the possible penalties for such a breach.

Key differences include:

- Increased rights for individuals, including: an expanded requirement for data controllers to obtain informed consent to the processing of personal data; the right for individuals to be 'forgotten' (i.e. for their data to be deleted); the right to data portability; and the right to access a copy of the data held on them free of charge.

- Data processors will be subject to many of the same requirements as data controllers – including the financial penalties for any data breaches.

- The requirement for data protection to be incorporated 'by design' – data protection must be at the core of all procedures etc, rather than just an add-on. In addition, data protection impact assessments must be undertaken when introducing any new technologies.

- The requirement to report data breaches that present a high risk to rights and freedoms within 72 hours; and for such breaches to draw one of two tiers of penalties, with the highest fine being up to the greater of 4% of the organisation's worldwide annual turnover or €20 million.

Overall, the emphasis is on: greater rights for individuals; increased transparency about how data is processed; the need to be able to demonstrate compliance with the requirements; and significant penalties for any breaches.

Data Protection Bill and Processing Without Consent

Following Royal Assent, this Bill will supplement the GDPR, even after Brexit. It defines, in a UK context, terms within the GDPR and introduces new criminal offences not present in the EU Regulation. There is an occupational pensions specific easement for processing personal data without consent subject to certain conditions.

The Information Commissioner's Office (ICO) – the overseer of data protection within the UK - will have a reinforced role and will be required to produce Codes of Practice in various areas, notably on data-sharing.

Both the eventual new Data Protection Act and the GDPR will need to be read together: there is provision for articles in the GDPR to be taken as if forming part of UK law.

Preparing for the GDPR

The starting point for any organisation preparing for the GDPR is likely to be a comprehensive review of internal data flows: where did the data come from, how is it held, where is it used and who is it passed on to?

Such a review will help identify which activities may need to be compliant with the GDPR, which processes may pose a particular risk and may even identify data items that are being held unnecessarily.

Having identified the processes that may be affected, organisations can then consider the grounds on which they are processing personal data. The GDPR sets out a limited range of grounds on which such processing can be undertaken and also requires the data subject to be notified of the basis on which their data is being processed. Under the DPA '98, many pension arrangements will be processing personal data on the basis of the consent of the individual – in some cases relying on 'implied consent'. Whilst 'consent' is still a valid processing ground under the GDPR, there are additional considerations because any such consent must be explicitly and freely given: it seems that it cannot be freely given where the data subject could not refuse to give consent without detriment to themselves. It may be difficult to argue that a pension scheme member would not suffer detriment if the scheme was unable to process their data, so relying on any individual's consent to the processing of their data is risky to say the least.

Data controllers should ensure that they understand the grounds on which they are processing individuals' data (which may vary for different processes) and may need to notify all members, before 25 March 2018, of the grounds on which their data is being processed.

Identifying the processes that may be affected and establishing (and notifying) the grounds on which individuals' data will be processed is only the starting point in preparing for the GDPR. Fortunately, the Pensions and Lifetime Savings Association (PLSA) has produced a free guide detailing the further steps that may be required.

For the next part of this Aries Insight, then, we will consider some of the other issues that the GDPR may pose for pension schemes and providers.

Data Retention Periods

Pension arrangements are long-term in nature – personal data may be held for well over 50 years to enable benefits to be calculated and paid out when due. Even once a scheme has discharged its liability for an individual member (for example, where benefits are transferred out or all benefits settled on death), schemes and providers will generally wish to retain the relevant data, to protect themselves against any possible subsequent queries or claims.

There is an existing requirement under the DPA '98 that data is not kept for any longer than necessary, and this requirement is carried forward under the GDPR. It must, however, be balanced against the statutory requirement [Regulation 14 of SI 1996/1715] to retain all scheme records for at least six years after the year to which the records relate and, where relevant, the guidance from the Pensions Regulator. For example, "*providers and trustees need to be aware that members sometimes have queries about their past contribution and transaction history, and they may require access to historic information for many years*" (TPR Record-keeping guidance, December 2008: Appendix 2). In addition, the FCA requires certain firms to retain some records indefinitely.

Most recently, the 2017 Money Laundering Regulations require trustees of an occupational pension scheme to maintain up-to-date records,

of beneficial owners of the trust, for five years after the final distribution is made.

Data controllers will need to consider their data retention policy and also establish how they would accommodate any request from an individual to exercise their new right under the GDPR for their data to be erased in certain circumstances (often referred to as the right to be forgotten).

Data Subject Access Requests

Under the GDPR, individuals have enhanced rights to request a copy of all the personal data that is held on them. The maximum time period for fulfilling such a request is reduced from 40 days under the DPA '98 to just one month. In addition, data controllers can no longer impose a charge for such a request (although it may be possible to charge for repeated requests).

To complicate matters, the GDPR envisions that a copy of the individual's data will be provided electronically, in a common machine-readable format. Data controllers will need to review and update their process for responding to any data subject access requests and should also consider whether there is likely to be an increased number of such requests once the GDPR takes effect.

Staff Awareness

A key component for the successful transition to the GDPR regime is staff awareness of the changes. Front-line, member facing staff need to understand not only the increased rights of individuals but also any changes to existing internal policies and procedures. Those responsible for developing internal procedures and processes may need to be actively engaged with any process reviews, whilst those responsible for data storage systems may need to review existing data security protocols.

As an introduction to the changes that are coming in, you may wish to circulate this Aries Insight to all staff who may be affected and also ask us about the Aries Pension System.

In addition, all staff should be familiar with the actions required where a potential data breach is identified and know who the organisation's Data Protection Officer is, where one has been appointed. Where there is no existing Data Protection Officer, careful consideration should be given to whether it is necessary to appoint one.

Reporting Breaches

Where a data breach is identified that is likely to "result in a risk for the rights and freedoms of individuals", the data controller must report this to the ICO within 72 hours of becoming aware of the breach.

In addition, if the breach is likely to result in a **high** risk to the rights and freedoms of individuals, the data controller may also need to notify the individuals affected by the breach.
To facilitate these notifications, data processors will be required to notify the data controller of any breaches of the GDPR as soon as reasonably possible.

Given the very significant fines that can be imposed for breaches of the GDPR, and the additional fines that can be imposed for failure to report a breach, pension schemes and providers may need to review not only their data security policies but also the breach reporting process. In turn, data controllers are likely to require assurance from any data processors that adequate policies and procedures are in place, to help the data controller demonstrate their compliance with the GDPR.

Data Protection Impact Assessment (DPIA)

Under the GDPR, a DPIA is required where a type of processing - particularly using new technologies - is likely to result in a high risk to individuals' rights and freedoms. This might include: evaluation or scoring, including profiling; automated decision-making with legal effects; systemic monitoring; and processing of sensitive data. This is not an exhaustive list; the Article 29 Working Party provides guidelines on whether processing is likely to result in a high risk, for DPIA purposes.

Also known as a privacy impact assessment, the purpose of such an assessment is to identify effective ways to comply with the requirements of the GDPR and ensure that data protection is integral to the development being undertaken – referred to in the GDPR as 'data protection by design'. The data controller must consult the ICO where the DPIA indicates a high risk in the absence of measures taken by the controller to mitigate the risk.

Resources To Help Prepare

The introduction of the GDPR poses major challenges to pension schemes and providers, who will need to be preparing for the changes well in advance of the implementation date in May 2018.

In addition to the PLSA guide and the information within the Aries Pensions System mentioned above, the ICO has produced a guide detailing the initial steps that organisations should be taking to prepare for the changes.

Further material is also available from the ICO website. The ICO has also produced a Code of Practice on privacy impact assessments. Whilst this is written in the context of the DPA '98 rather than the GDPR, it remains a useful resource.

Summary

The introduction of the GDPR represents the biggest change to data protection rules for 20 years and, whilst it may be all too tempting to simply pull the duvet over your head and try to ignore it, pension schemes and providers need to engage with the changes as soon as possible to ensure that their organisation is fully compliant – and can demonstrate its compliance – in time for the 25 May 2018 deadline.

Did you find this Aries Insight useful?

If so, then why not share it with your colleagues and let them know that more information is available from the Aries Pensions System.

If you have any suggestions for topics that you would like to see covered in a future Aries Insight, then please let us know. We cannot promise to cover every topic that may be suggested however as always we will do our best.

Aries Insights are produced for Aries Members by Aries Insight to highlight key legislative changes and other topics of interest. ***As they are only short articles, they cannot always cover every aspect of the topic being discussed and must not be considered as legal or financial advice.***

All Aries Insights are intended to reflect the position as at the date the Insight was issued. Please consider the possibility that the relevant legislation may have changed since an Insight was issued.

Aries Insight - November 2017