REGULATION

Ahead of the game

With the introduction of the GDPR fast approaching, Talya Misiri discusses the key elements of the regulation, what trustees will need to do to prepare their data and the consequences of non-compliance

WRITTEN BY TALYA MISIRI

Against a backdrop of political and economic uncertainty, distrust and threatening cyber-attacks, the need to be in control of data is more crucial than it has ever been. The European Union's General Data Protection Regulation (GDPR), set to be introduced in May 2018, has been, therefore, hugely welcomed.

The GDPR will replace the previous EU 1995 Data Protection Directive (DPD) and will apply to all 28 European Union member states, and increases the scope of the 1998 UK Data Protection Act (DPA).

The new regulation will continue on from the now-outdated Data Protection Directive. The provision will involve specific and more defined rules around personal information, how it is used, the consent needed, how long data can be kept for and stricter penalties for abusing or breaching the rules of the regulation.

While data laws may have been viewed as more of a guideline in the past, the introduction of GDPR means that "this *[data protection]* is now a 'must have' rather than a 'should do' as it may have been viewed historically", states Russell Scanlan operations director Andy Jenkins.

Purpose

The key purpose of GDPR can be attributed to two main areas: heightening the level of data protection to prevent fraud and data scams, and moving the overall control of personal data back to the owner.

"The GDPR will strengthen and unify data protection for individuals within the EU," says DLA Piper employment and pensions group partner Claire Bell.

The GDPR has been introduced in order to bring data protection up to date in today's cyber world. In light of recent data scams, the new regulation has set much more defined, specific rules to ensure that data is safeguarded.

The importance of personal ownership is also a key factor that sets the GDPR apart from its predecessor, the DPD.

The aim is for the individual to allow access to their personal data rather than passing on the ownership once they have submitted their personal information. Under the regulation members will also have the right to access detailed information from trustees regarding the processing of their data and what data is held.

Jenkins explains that the "'opt out' approach must be replaced by the 'opt in' approach" regarding the provision of personal data to the scheme.

Preparation

Pension schemes across Europe are now being urged to put the necessary data preparations in place before the regulation's launch next year. Jenkins notes that: "The current feeling is that if a business is fully compliant with the (UK's) DPA, it should be at least 80 per cent compliant with GDPR."

While the GDPR does share a considerable deal of commonalities with the previous data protection directive and the UK's DPA, it does not mean that UK schemes should become complacent and not act in preparation for the new regulation.

It is advised that trustees initially carry out an information audit in

[DATA PROTECTION] **IS NOW A 'MUST HAVE' RATHER THAN A 'SHOULD DO' AS IT MAY HAVE BEEN VIEWED HISTORICALLY**

order to fully understand their data. They must check what information is being kept, why, how long for and whether it is still required.

Furthermore, another key area in which pension schemes must work on under the GDPR is consent. Prior to this it has been noted that schemes assume member consent simply by them joining the pension scheme. However, the new regulation places greater emphasis on schemes directly acquiring documented formal consent from their members.

Privacy notices, the information provided to members explaining how their personal data is being used, will also need to be revised. The GDPR requires privacy notices to be extended, including information such as how long their information will be stored for and the rights the member has in relation to their personal data. This must be communicated in a simple, clear way.

In addition to these administration changes, larger-scale organisations and businesses will be expected to appoint a data protection officer to ensure full compliance. This person will oversee data policing policies, compliance of new digital assets under GDPR and will also assess risks, train employees, carry out cyber audits and report any breaches.

According to the Information Commissioner's Office (ICO), a data protection officer must be appointed if you are a public authority or carry out large scale systematic monitoring of individuals.

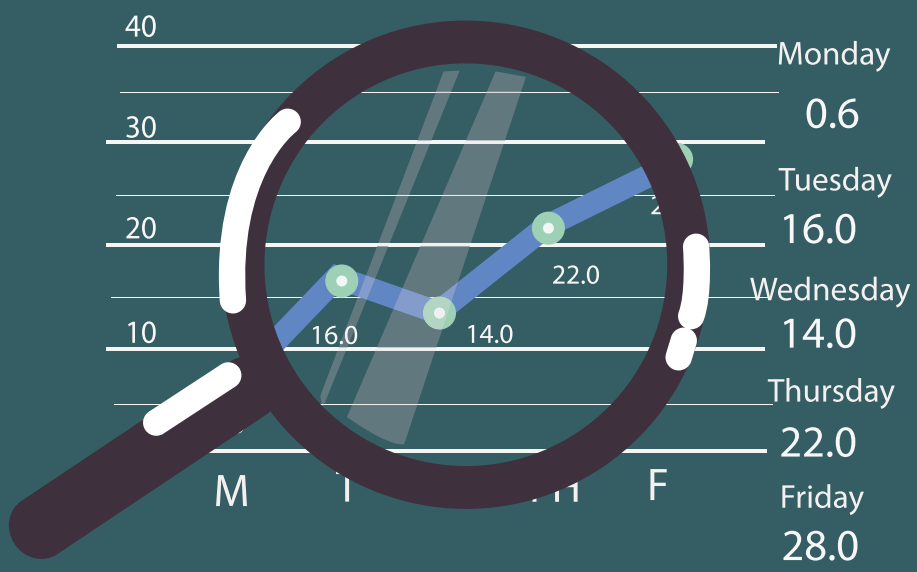
Furthermore, communication between all parties involved in governing and managing the scheme is crucial. Trustees should work in cohesion with employers, as well as administrators and advisers, to discuss how they are preparing for the regulation and how their roles will change once the GDPR comes into force.

Breaches

Rules under the GDPR are also much tougher than the DPD when it comes to compliance and data breaches. Failure to comply with the regulation will result in companies facing penalties of up to €20 million or 4 per cent of annual global turnover, whichever is higher.

Trustees are ultimately liable for any breaches of the GDPR, whether it be a result of their own actions or that of their data processors. With this heightened pressure and demand on trustees, they are encouraged to

FAILURE TO COMPLY WITH THE REGULATION WILL RESULT IN COMPANIES FACING PENALTIES OF UP TO €20 MILLION OR 4 PER CENT OF ANNUAL GLOBAL TURNOVER



ensure that they are "adequately protected under contractual arrangements", Bell adds.

The rules have also been amended regarding data breach notification requirements. Trustees and data controllers are required to notify the ICO of personal data breaches "without undue delay". The ICO must be informed of the breach within 72 hours of it being identified and each will be individually assessed on a case-by-case basis.

In addition to this, affected individuals are also expected to be directly notified and also without delay if it is likely to abuse their rights.

Nonetheless, these stricter guidelines than the previous DPD regulation and heftier penalties can help to encourage better record keeping overall.

Bell explains that: "The high levels of fines and penalties imposed on data controllers who fail to comply with GDPR will encourage higher levels of internal accountability and record keeping."

Although the GDPR necessitates a much greater amount of admin from trustees and data controllers than the previous directive, the new regulation will lead to developed communications, data transparency, tightened personal information management guidelines and ultimately the safeguarding of unauthorised data transfers or fraudulent interferences. In light of recent cyber scams and attacks, it is essential that the European pensions space tightens its data controls to ensure all personal information is protected.

RSM technology risk assurance partner Steve Snaith concludes: "Although GDPR is a welcome attempt to curb growing fears around how companies use and manage personal information, the new framework will drastically affect the future of stored personal data and increase company accountability. Pension schemes must make sure they are ready for what lies ahead and not get caught out, as the financial and reputational risk could be significant." ■

Brexit and GDPR

With the continued Brexit negotiations following the UK's decision to leave the European Union, British pension schemes are likely to question what GDPR will mean for the UK.

To address this directly, the UK's full compliance with the European data regulation is still largely obligatory. Addleshaw Goddard legal director and head of the data and information team Toni Vitale confirms: "Trustees will need to prepare for GDPR compliance notwithstanding Brexit. If trustees have their person data processed in other EU member states, they will have to continue to comply anyway."

It is expected that after the UK's official departure from the European Union, GDPR will be entrenched into UK law via the Great Repeal Bill.

The ICO has suggested that the UK is likely to want to keep the European regulation in place, in order to allow for cross-border transfers and maintain the data of European citizens.