REGULATION

A necessary measure

European Pensions explores what schemes should have in place in preparation for the EU's upcoming General Data Protection Regulation, how it differs to regulations that were in place prior to introduction of GDPR, and the penalties for non-compliance

WRITTEN BY PETER CARVILL, A FREELANCE JOURNALIST

If the issue of how data is kept and managed had not been sitting at the forefront of the public's mind, it planted itself firmly there in March. That was when tech giant Facebook found itself swimming in hot water after the UK's Channel 4 and *The Guardian* revealed that the data of 50 million people had been harvested – apparently largely without their consent – by Cambridge Analytica, a company specialising in political campaigning and working to swing the results of elections and referendums.

Facebook's subsequent loss of reputation and the repercussions it felt came hard and fast, with the stock price of the company falling 14 per cent in a week, and the brand suffering a $80 billion fall in value.

GDPR principles

The social network's troubles come at the same time as the EU's General Data Protection Regulation (GDPR) is about to come into force following a two-year implementation period. Superseding the Data Protection Directive (DPD) of 1995, the GDPR comes into effect on 25 May.

In a white paper, tech giant Microsoft said: "While the GDPR preserves many of the principles established in the directive, it is a much more ambitious law. Among its most notable changes, the GDPR gives individuals greater control over their personal data and imposes many new obligations on organisations that collect, handle or analyse personal data. The GDPR also gives national regulators new powers to impose significant fines on organisations that breach the law."

It is a regulation that is built upon the six principles of transparency, fairness, and lawfulness in the handling of data; limiting the processing of said data to specified, explicit, and legitimate purposes; minimising the collection and storage of personal data; ensuring the accuracy of personal data while enabling it to be erased or corrected; limiting the storage of personal data; and ensuring the security, integrity, and confidentiality of that data.

The GDPR is applicable to all organisations, regardless of size and industry, if they hold the data of any citizen in the EU. It is not a weak piece of legislation: the penalties for non-compliance are harsh, with a maximum fine for serious infringements of 4 per cent of an organisation's annual global revenue, or €20 million, whichever is the greater.

Trafalgar House director Dan Taylor outlines the difference between the GDPR and the regulation preceding it. "What it relies on," he says, "is for you to have evidence of the standards you had. While pension schemes may

think they were complying, you now have to document and prove. That's the key difference."

Application

In applying the GDPR to their business models, schemes need to look at what they communicate to their members, and how. RSM Risk Assurance Services' partner Steve Snaith says that members will be looking for assurance that their data is being properly protected. "From their point of view," he says, "it's all about data privacy and protection. The organisations need to have safeguards in place and make sure that the right governance is there to protect their customers."

UK professional trustee firm, PTL, managing director Richard Butcher goes further. Although he says that schemes have a legitimate interest in holding data on members, he says that they should be sending those members a privacy notice, outlining the data that the scheme holds, the reason it is held, and what those member's rights are in relation to that data. "The general sense," he adds "is that consent can be obtained at the point the data is used, although there are still a number of unanswered questions in relation to this, e.g. sensitive personal data on beneficiaries supplied on an Expression of Wish form."

That said, it appears most feel they are adequately prepared for 25 May. Software company Lever recently conducted a survey of 500 professionals and found that 70 per cent felt that they had prepared adequately.

While Butcher acknowledges that a lot of progress has been made towards compliance, he says there are still concerns and worries. "Are schemes ready? Probably not entirely, although this is, in part, because a) the final regulations have yet to be produced and b) what is in the public domain is open to interpretation."

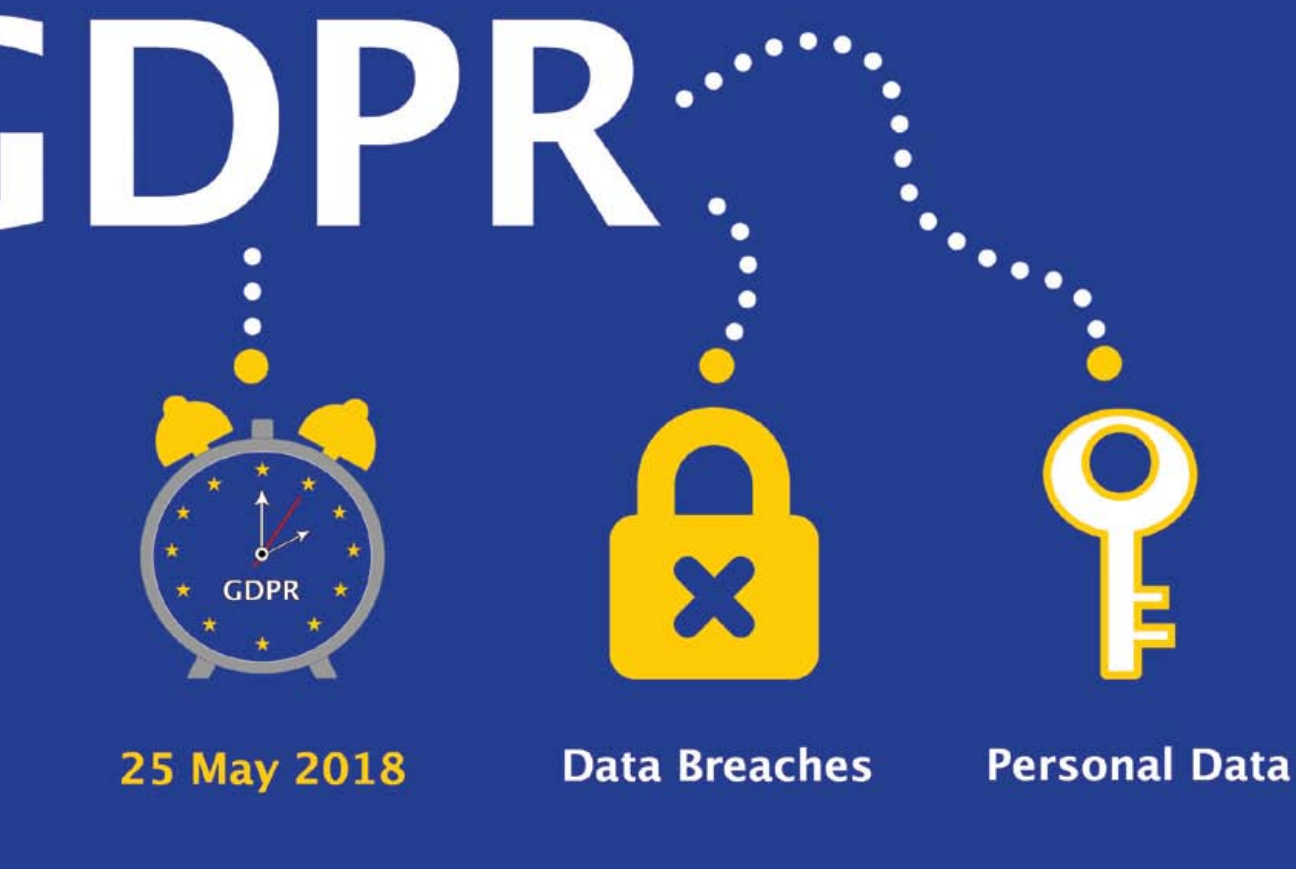
PENSION SCHEMES SHOULD NOT ASSUME THAT ALL THEIR INFORMATION IS WELL-TRACKED OR KEPT IN ONE PLACE

But as implementation looms, many organisations – not just pension schemes – are rushing to ensure that they are ready. However, pension schemes should not assume that all their information is well-tracked or kept in one place.

Snaith explains: "Pension schemes need to understand is the scope of the information they hold, whether it's digital, paper, spreadsheets, etc… They need to have mapped that out and understand what it is. That should be – and should have been – the first step. The risk is that there's data out there that's not been fully documented and may not be as protected as other information. Knowing where it is is crucial."

Taylor seconds this, saying the most-important aspect of GDPR is that pension schemes across the continent know with certainty where the data they have collated is kept. It is, he says, 'absolutely essential'. "If you look at pensions administrators," he adds, "there's an assumption that the data is all in one location. But they might have cloud-based services, mortality screening services, trading services, printers, contact with actuaries. So understanding that data flow and its location is more complicated than people realise."

There was a two-year transition period for organisations to implement the changes needed to comply with this regulation. At the point of writing, temperatures are rising for organisations not sufficiently prepared for GDPR.



After all, nothing focuses the mind better than a deadline.

"My impression," says Taylor, "is that most pensions companies will be okay. It's doubtful that scheme providers will know everything, and have it nailed down in time. But I think most will have done enough to be protected and prepared."

However, he says he worries about the small schemes that may have not prepared at all. Some providers, he says, are "still waking up to it".

Ultimately, the world has changed in the past 20 years. Data leaks and hacks have become commonplace, as has high-profile cases of social networks and media companies having huge breaches of data. So while the medicine may taste bitter, it is a necessary measure. After all, says Taylor, "It's difficult but it's the right thing to do. And people will agree with that. We've changed so much since 1998 – the time is right for this kind of change." ■

UK post-Brexit

On 23 June 2016, the UK held a referendum to decide on whether the country should remain part of the European Union. As a consequence of the result – a 52 per cent majority in favour of leaving – the UK is going through the process of extricating itself from the EU. This leaves the country in a strange position regarding GDPR. According to the EUGDPR, a website run by technology company Trunomi, "If *[companies in the UK]* process data about individuals in the context of selling goods or services to citizens in other EU countries then you will need to comply with the GDPR, irrespective as to whether or not you the UK retains the GDPR post-Brexit."

However, if activities are limited to the UK, says Trunomi, then the position is a murkier one. They say, "The UK government has indicated it will implement an equivalent or alternative legal mechanisms. Our expectation is that any such legislation will largely follow the GDPR, given the support previously provided to the GDPR by the ICO and UK government as an effective privacy standard, together with the fact that the GDPR provides a clear baseline against which UK business can seek continued access to the EU digital market."