GDPR – one year on

GDPR caused lots of disruption prior to its implementation, but how much of an impact does it have now over a year on from its launch? Chris Tagg explains

GDPR arrived in May 2018 on the back of a long build up filled with a combination of excitement and dread. The pensions industry saw its introduction largely as evolution, building on existing DPA legislation, rather than anything brand new and onerous to comply with. There was, though, obvious work to be done to ensure compliance – like data maps and privacy notices, etc – and a soft(ish) deadline to focus trustees' minds on the issue.

Let's take a look at what the immediate impact was and how that has evolved one year on…

A hard slog – data maps/privacy notices

There were various interpretations on what these documents should look like and when they needed to be produced. At a high level, data maps set out what data is to be held and used, why and by whom, while privacy notices summarise this information for individuals to whom said data relates.

There was a general acceptance that a plan was required to be in place by May 2018 but actual work and adoption/issue of the documents could follow. The majority of these documents that are now in place follow similar templates (almost certainly based on legal advice). Review and updates are now in place on business plans and processes have been updated to ensure appropriate publication and circulation to relevant parties.

A non-event? – contract updates

There are a lot of service providers in the pensions industry, which meant updating contracts to reflect new legislation. As contracts are updated from time to time anyway this was absorbed with little fuss, as expected. The main changes have been updates to terms of business and new GDPR schedules being added, introducing new relevant definitions, etc.

A little tinkering – data controllers/processors (and sub-processors)

Not much changed in these defined roles but some clarity was needed to ensure individuals and organisations understood their roles under GDPR. Given supply chains are often longer than just directly-contracted parties, there was some work to do to ensure data controllers understood how their data was being processed and by whom. Service providers reviewed their own contracts with suppliers, to ensure they were GDPR-compliant and to provide comfort to their own pension scheme clients.

Increased awareness – data sharing, purpose limitation and deletion

This is a prime example of evolution rather than revolution; data security requirements are no tougher under GDPR than they were under DPA 1998 – they were just brought into sharper focus by increased fines as punishments for breaches. There has, though, been a proliferation of secure file transfer mechanisms (websites and portals, etc) both between professional firms and with pension scheme members.

Data controllers have become much more aware of the data they hold and, importantly, why they hold it and how it should be used. A perverse impact from this has actually been a proliferation of the data items pension schemes hold in relation to their members; especially in relation to endgame projects.

The yin to the increased data volume yang is redundant data. The majority of firms in the advisory space have been looking at data retention policies and have begun the process of deleting and/or destroying data for lost clients. This should not be a big issue for schemes as the data is likely already to be held in other formats (eg scanned documents being held electronic or member data being on a new administrator's system) but data controllers should be aware this is happening.

Additional work volumes (and cost) – SARs

The big unknown with GDPR was data subject access requests (SARs). Members suddenly had greater freedom to find out what data organisations hold for them. Would the data floodgates open and what would the associated burden be on data controllers/processors?

There has not been the feared volume of requests. SARs tend to be received where there is either cause for concern about security (perhaps in light of bad press) or a complaint is being raised. Additional workloads are therefore small but the inconvenience caused by timescales for complying with requests means they are complex and costly.

Data is almost certainly more secure now than in the pre-GDPR world and awareness has certainly been raised amongst scheme members which was, I think, the point. As with a lot of developments in the industry, GDPR has been adopted (even embraced?) very quickly and is now part of normal life. There are elements of additional work required day-to-day, but these are now second nature and not a significant burden.

Written by PASA board director Chris Tagg