GDPR
has it been a year already?

By Katy Harries,
Senior Associate, Sackers

It's hard to believe that nearly 12 months have passed since the General Data Protection Regulation (GDPR) came into force on 25th May 2018. We were told back then that this was only "the beginning, not the end"; so is an end now in sight?

What's still to do?

Each pension scheme will be at a difference place in terms of GDPR compliance. For example, some schemes have already had to deal with a large number of 'subject access requests' (where members ask to see their personal data), whereas some haven't had any at all. Some will have agreed contractual terms with their key providers, but others may still be struggling on that front. These different experiences mean there is no 'one size fits all' approach to GDPR compliance. However, on the whole, the following are key areas that pension schemes should be focussing on:

1. Contractual terms with other providers

Data controllers (including trustees of pension schemes), are required to have GDPR compliant contractual terms in place with all their data processors. Many trustees have found this process long and drawn out. Given the risk of sanctions for not having GDPR compliant terms in place, trustees must continue to focus on getting terms agreed with their data processors as soon as possible.

2. Dealing with data subject access requests

Although individuals already had rights to access personal data held about them under the old regime, they are now much more aware of their rights. The number of requests has increased dramatically under GDPR. With only a month to respond to a subject access request, pension schemes should put processes in place for dealing with this type of query. When putting their approach together, trustees should think about:

+ **how to check the identity of the member**
+ **making sure any third party has appropriate authority from the member**
+ **clarifying the level and detail of information required**
+ **how to present the personal data to members.**

As the scheme administrator will hold the member records, trustees should work with them in setting up a process for responding to these requests.

3. Dealing with breaches

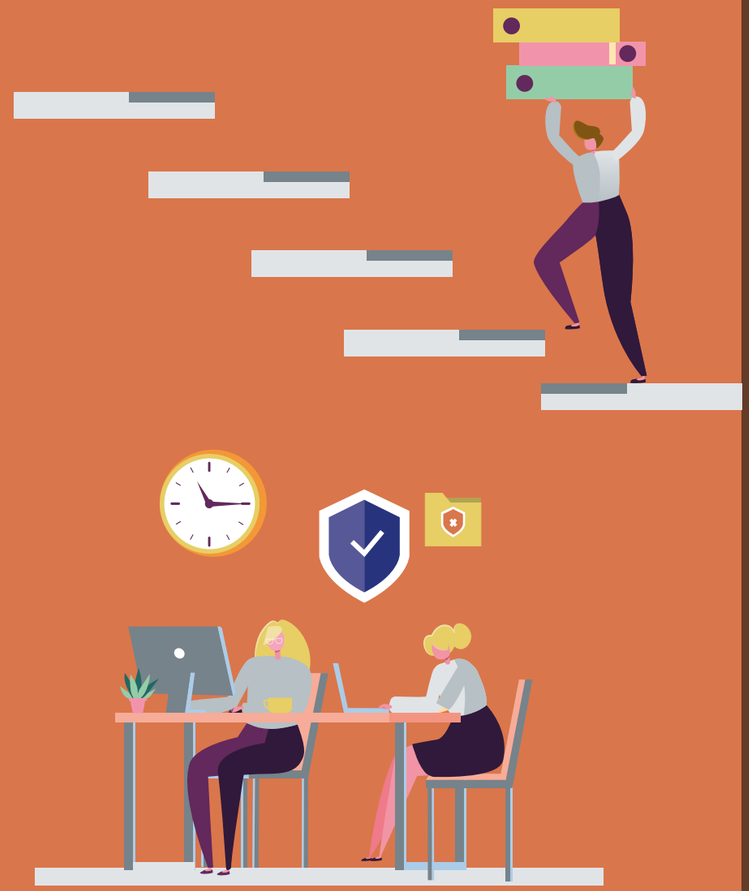
Even having a flawless data protection policy in place and properly implemented cannot, unfortunately, prevent breaches from happening, whether due to a malicious attack (e.g. viruses) or genuine human error (e.g. loss of a portable device containing personal data).

Where there is a breach, trustees may have to report it to the Information Commissioner's Office (ICO), and to the individual concerned, depending on the seriousness of the breach. A data controller is required to report a serious personal data breach to the ICO within 72 hours, where feasible.

In order to handle a potential breach efficiently, it is crucial to have a proper process in place. Trustees should consider the key individuals involved (e.g. who should be contacted initially, who will investigate the breach), and, where the breach is by a provider, how to work with that provider in investigating and reporting that breach.

4. Record keeping

In the run-up to May 2018, pension schemes were busy carrying out audits on the personal data they held. As the GDPR requires all controllers and processors to maintain a processing record, trustees should check that the relevant information has been pulled together for this purpose. The original personal data audit will provide a platform for this but, given the sheer volume of personal data held by schemes, this is proving a challenging area. The administrators will again play an essential role.



What's still to come?

GDPR compliance is a new area for all data controllers, not just for pension scheme trustees. It will take time for best practice to develop and to see how the ICO will enforce the GDPR. Key areas on the horizon include:

1. Brexit

At the time of writing, there was still no decision on whether we would leave with a deal, with no deal, or even what the eventual Brexit date would be. The ICO and the government have confirmed that GDPR will remain law post-Brexit, regardless of the circumstances of our departure. However, pension schemes should keep an eye on the position regarding transfers of data between the UK and the EU. Whilst the government has confirmed that it will continue to allow the free flow of data from the UK in the event of a no deal, transfers from the EU to the UK will need to be subject to the same 'appropriate safeguards' that apply to 'third countries'.

2. Best practice

The ICO has been publishing guidance on various aspects of the new data protection obligations and will continue to do so. As time goes on, the guidance, together with practical experience of pension schemes, should all help 'best practice' to develop. On the technological side, security measures will continue to improve. Trustees will need to review and update their processes and policies to keep in line with these developments.

3. Monitoring data processors

As well as keeping their own processes under review, trustees will also need to monitor their data processors, to check that they are processing data in a GDPR compliant manner.

Is the end in sight?

We expect the initial stage of updating processes and contracts to be well underway, and hopefully the end of this stage will be in sight for most trustees. However, trustees' data protection obligations are ongoing, as you can see from the list above. So, whilst you can give yourself a pat on the back when the initial stage is complete, don't skip off into the sunset just yet.