AN INTRODUCTION TO GDPR

A new EU directive on data protection will come into effect from 25 May 2018. The General Data Protection Regulation (GDPR) will replace the existing EU directive, which is now over 20 years old.

Despite the UK's decision to leave the EU, the UK is expected to implement the GDPR in full. In fact, its principles were included in the Data Protection Bill that was announced in the Queen's Speech. The GDPR and the Data Protection Bill will make sure the EU and the UK have a data protection regime that's fit for the 21st century.

Trustees are responsible for controlling their members' data – under the GDPR, they're called 'controllers'. Since all trustees will need to comply with the new regulations when they come into force next May, it's important that trustees start thinking about what the GDPR means for them.

THE PURPOSE OF THE GDPR

The purpose of the GDPR is to bring together different data protection procedures, and strengthen how those procedures are enforced.

It will make sure individuals have more rights – one of the most significant changes is to how individuals give their consent to have their data processed.

It will also introduce new rules for data processors, including pension scheme administrators.

And if trustees don't comply, they could face significantly increased fines.

THE PRINCIPLES OF THE GDPR

The six principles of the GDPR cover the same ground as the eight principles in the current EU directive. Their implications for a trustee are:

1. You should be processing personal data legally, fairly, and in a transparent manner.
2. You should only use personal data for the purpose for which it was collected.
3. You should limit the personal data to what's needed, making sure it's adequate and relevant.
4. You should make sure personal data is accurate and kept up-to-date. If you find out that any of the personal data is inaccurate, you must take every reasonable step to make sure it's deleted or corrected as soon as possible.
5. You should keep personal data no longer than is necessary for the purposes for which the data are processed.
6. You should process the personal data securely. This includes protecting it against unauthorised or illegal processing, and against accidental loss, destruction or damage.

DATA SUBJECT RIGHTS

Understanding data subject rights is important as they form a cornerstone of the GDPR. Trustees and service providers must be able to identify when a data subject wants to exercise their rights and take prompt, controlled action.

Some people equate data subject rights with subject access requests. This is understandable, as this is the most commonly right exercised by pension scheme data subjects. However, it is only one of many rights. Others include:

- The right to rectification
- The right to be forgotten
- The right to restrict processing
- The right to data portability
- The right to object
- The right not to be subject to an automated decision.

SOME QUESTIONS FOR TRUSTEES TO CONSIDER

1. Do you know all the parties who process your data?
2. How will you commincate changes in your Privacy Notice to your members?
3. When do you see individual member data and can this be anonymised?
4. What is your policy on how long to retain data?
5. How do trustees receive meeting papers and exchange information between themselves?
6. What is your sponsor doing to comply with GDPR – can you work together?