GDPR Trustee Handbook

May 2018

GDPR and how it affects you as a Trustee

The EU General Data Protection Regulation (GDPR) comes into force on 25 May 2018 bringing about fundamental changes how personal data is held and processed. It will be applicable throughout the EU, and Brexit will not affect it's implementation in the UK. A trust is categorised as an entity in it's own right and is subjected to the new regulations and compliance. As you have a trust, you will be affected by GDPR and it is important that we implement a compliance process for your scheme.

This is what our GDPR team intends to do to help ensure your trust is compliant:

- update the privacy notices
- review the processes of record keeping and evidencing
- ensure you have agreements in place with third party processors – e.g. the scheme bankers
- ensure you have processes to comply with the Subject Access Requests and data portability requests – for example, where you have a sponsoring employer linked to the Trust / SSAS
- ensure you are equipped to detect and deal with the data breaches
- seek individual consent where necessary for processing

Trustees are the "data controllers" responsible for the compliance with the new GDPR Regulations, so it will be your duty to ensure that you have considered cyber security issues and any potential weaknesses the data may be exposed to. As the registered administrators to your Scheme, you have appointed us to deal with your scheme GDPR requirement. Therefore, we depend on you as Trustees to keep us up to date with changes in how data is held and who holds it. We will act as your data compliance officer in relation to the Scheme, notify and deal with the ICO and any changes over the coming 3 years.

What we need to do now

We will prepare and send to you an information form which contains all the parties who have access to your pension scheme data – we will ask you to confirm that the data is relevant and accurate and to insert any parties who are not on this document and therefore we do not hold a record of.

We will also send you an information document on key data held which covers the sponsoring employer, the trustees, members and beneficiaries. We would ask that you provide us with any updates so that our data held is complete and accurate. These forms will help us to carry out the implementation of satisfying your Scheme's GDPR requirements.

Areas of attention

If you haven't done so already, we will help you implement the following:

- update the privacy notices
- review the processes of record keeping and evidencing
- ensure you have agreements in place with third party processors
- you have processes to comply with the Subject Access Requests and data portability requests
- you are equipped to detect and deal with the data breaches
- seek individual consent where necessary for processing

Trustees are the “data controllers” responsible for the compliance with the GDPR, so it will be your duty to ensure that you have considered cyber security issues and any potential weaknesses the data may be exposed to.

Privacy notices

The changes in privacy law mean additional information requirements for data subjects. Data controllers must be clear and specific when explaining how the data will be used, including:

- source of dataand if third party processors used, list of such processors and clear indication of their involvement;
- legal basis for the processing;
- if processing is reliant on the individual consent, the individual must be informed of the right to withdraw the consent at any time;
- if special categories data is being processed, the notice must specify the conditions of processing the special categories data;
- privacy notice must include individual’s right to access his/her data and the right to data portability and individual’s right for the data to be rectified or erased.

Legal and regulatory requirements must still be adhered to when ensuring individual’s rights. When complying with one individual’s rights the controller must ensure not to infringe other individual’s right to privacy.

Subject Access and Data Portability Requests

Subject Access requests already exist under the current legislation, however few requirements are changing under the GDPR:

- The information has to be provided within one month (currently 40 days), it can be extended to two months under exceptional circumstances;
- the information must be provided for free of charge;
- the individuals must be told for how long their data will be stored, or criteria for deciding the period of storage;
- individuals have a right to restrict or pause processing;
- individuals must be told about the rights to have their data corrected and deleted.
- Individuals also have the right to request their data file in an easily accessible standard format for data portability purposes under the GDPR

Record keeping

Increased emphasis will be on record keeping and the trustee's ability to demonstrate compliance. This can be achieved by having detailed and documented procedures in place. The same requirements apply to pension scheme administrators. Exemptions are in place for companies with less than 250 employees, but this is unlikely to apply to pension scheme trustees and administrators due to special categories data processing that is involved with managing pension schemes and Trusts. It is crucial that the trustees ensure adequate training for the people involved in any processing procedures.

The key information to be recorded includes:

- The name and contact details of the data controller (and joint controllers if applicable);
- The details of the data protection officer (if applicable);
- The purpose of data processing;
- The legal basis of data processing;
- The categories of data subject;
- The categories of personal data that is being processed;
- Any parties that the personal data is being disclosed to or shared with and the reasons for disclosure/sharing;
- If data is being transferred to a third country, details of such transfers and safeguards implemented to protect the data;
- Detailed timescales (regulatory or processing related) for keeping various categories of data
- Detailsof organisational and technical measures applied to safeguarding the data
- Record of all contracts between data controller and data processors (if applicable)

Third party processing

Legal definitions define clear roles and responsibilities under the GDPR. Trustees are the data controllers, administrators as well as other service providers will be the data processors. The data processors as well as controllers will be responsible for the data and have direct obligations to comply with the GDPR. Both controller and processor will be liable for any claims from individuals in the event of data breach depending where the breach occurred. It is therefore compulsory to have a contract between the data controller and processor to set specific terms in order to ensure compliance measures are in place to safeguard personal data.

The content of the contracts is set out in GDPR and includes:

- The term of processing, its nature and purpose;
- the subject matter and type of personal data and categories of data subjects that are being processed;
- terms of compliant processing that sets the data subjects rights as a priority; and reporting to the trustees on request, demonstrating compliance;
- terms specifying how the data is returned or destroyed after the contact has expired
- terms prohibiting sub-contracting without trustee's written authorisation; all sub-contractors must be subject to the same terms of processing as the processor
- Contracts will be required for all other linked providers such as marketing service providers, independent financial advisers, annuity providers, protection planning services providers etc.
- Actuaries are likely to be considered data controllers in their own right.
- Further restrictions are placed on schemes where administration is outsourced outside EU.

Penalties

The penalties for non-compliance with the GDPR are designed to be proportionate, effective and dissuasive.
There will be two tier fine system in place depending on the severity of the breach and evidence of measures taken by the data controller to mitigate risks of a data breach.

Top tier breaches will be up to €20M or 4% of annual global turnover, whichever is higher.
Lower tier breaches will be up to €10M or 2% of annual global turnover, whichever is higher.

Consent

Rules around consent are substantially stricter under the GDPR, however it is important to differentiate between circumstances when consent is required, as there are other lawful grounds for processing. This is very much the case for pension schemes, as the services are provided in order to fulfil a contract. Other lawful grounds for processing are when the controller or processor is:

- complying with legal obligations;
- protecting the vital interests of an individual;
- acting in the best interest of public;
- for the purposes of acting in the best legitimate interest of the controller or the processor (this must not conflict with the data subjects right to privacy and must not adversely effect their rights).

Explicit consent will be required, in addition to lawful grounds for processing, when dealing with special categories data. For example trustees dealing with drawdown on the grounds of ill health must have evidence of consent being given for processing. Individual giving consent, can take it away at any time does not necessary apply in this scenario, as the scheme must comply with the law. Review of the documents is highly recommended to ensure consent is requested, obtained and documented appropriately.

Data Protection Impact Assessment

Before processing data that may carry a high risk for individuals, data controllers must carry out a DPIA. For example when processing large scale special categories data, or carrying out systematic monitoring of individuals and making decisions that can affect them based on the results of such monitoring.

Data Protection Officer

A DPO is required for certain circumstances. If processing is carried out by a public body; if the processor is involved in systematic and large scale monitoring of individuals; if the processor's core activities involve large scale processing of special categories data.
We have sought clarification from the ICO in relation to where they see DPO requirements fitting with the pension schemes; it would be seen as best practice for pension schemes to appoint a DPO. Further clarification will be available following the Data Protection Bill being released.

Data Breaches

In the event of a personal data breach, GDPR has placed additional requirements on data controllers. The breach must be reported to the ICO within 72 hours from being detected, if there is a threat to the data subjects rights and freedoms. The form for data breach reporting is available for download on the ICO website;

- the form must contain details of number of individuals affected, categories of data involved, likely consequences of breach and measures taken to mitigate the effects of the breach.
- If there is a direct risk to the individuals concerned, for example in the event of credit card details being lost, those individuals must be notified directly by the data controller.
- If the breach is resulting from the actions of the data processor, they must notify the data controller at the earliest opportunity after becoming aware of the breach.

The ten-point Sackers GDPR checklist

1. Audit your personal data: Under the GDPR, "personal data" is any information (whether opinion or facts) relating to an identified or identifiable living individual. As the ultimate responsibility for member personal data rests with the pension scheme's trustees, they are "data controllers" for this purpose. Trustees therefore need to make sure they know what personal data they hold, why they hold it, who else has access to it, how long it has been held, and whether it is still needed

2. What grounds do you have for processing personal data? For the processing of non-sensitive personal data to be lawful, at least one of six conditions must be met. Trustees therefore need to decide the basis (or legal grounds) on which they process scheme member personal data. Where consent is used as a basis for processing members' personal data (e.g. where sensitive personal data is being processed), the procedures for obtaining consent should be reviewed and updated

3. Update your contracts: Trustees will need to have a binding contract in place with any data processor whose services they engage, which will need to address a number of key points, including the subject matter and duration of the processing, the nature and purpose of the processing, the types of personal data involved, and the categories of individuals on whom it is held

4. Communicate with members: The GDPR will introduce additional requirements affecting the provision of information to members. Trustees will need to issue revised information notices (also known as privacy notices). Where trustees are joint data controllers, for example with the scheme actuary, the trustees may wish to prepare a joint privacy notice

5. Do members know their rights? Trustees need to tell members how their personal data is processed and ensure that members are fully aware of their rights in relation to the personal data that is held, such as the right to be forgotten and to have inaccurate personal data corrected. Trustees should ensure that their processes (and those of their advisers) are ready to deal with data requests from members

6. Review your policy: The trustees' data protection policy will be the main document for recording how they look after personal data in relation to their scheme, reflecting key decisions taken and procedures put in place to meet GDPR requirements. The content and structure will vary, but should aim to cover certain points as a minimum in line with record keeping requirements

7. Do you need a data protection officer: Both data controllers and processors will need to appoint a data protection officer (DPO) in certain circumstances, such as where their core activities involve "regular and systematic monitoring of data subjects on a large scale", or consist of large scale processing of sensitive personal data. Whilst it's unlikely that occupational scheme trustees will need to appoint a DPO, all schemes should assess whether they need one with input from their legal advisers and document their conclusions

8. Understand your role: Key to GDPR compliance is ensuring you understand what is required under the new rules. Talk to your legal advisers about how they can help

9. Be ready to demonstrate compliance: A new principle of accountability requires data controllers to be responsible for, and demonstrate compliance with, the data protection principles. Trustees should become familiar with the steps needed to fulfil their obligations

10. How well protected are you? Trustees should check what protections may be available to them in the event of any regulatory fines from the ICO or compensation claims from individuals arising from a data protection breach. As not all trustee insurance policies will cover such claims, it is important trustees check with their legal advisers the extent of any cover