Burges Salmon
Pensions Law Summary
Data Protection (GDPR) and Pension Schemes

Scope and Summary

This note provides a practical summary of data protection obligations for pension scheme trustees as at September 2021.

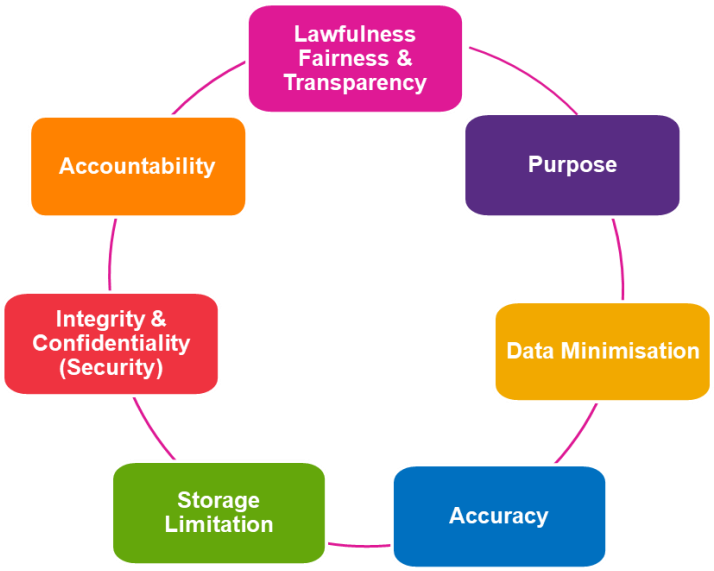
Key takeaway points include:

- The data protection regime (which changed dramatically in 2018) was not drafted with UK occupational pensions schemes in mind – it can therefore be complex to apply to pension schemes.
- The obligations are onerous and penalties for non-compliance in theory are severe.
- Trustees control and process significant amounts of personal data for members and beneficiaries and so will wish to ensure compliance. They may also be targets for cyber criminals seeking to access and use that data.
- Compliance is an ongoing obligation and so should be considered routinely.

Legal Position – Summary

The UK's data protection regime is governed by the retained EU General Data Protection Regulation (as the UK GDPR) and the Data Protection Act 2018, plus parallel and related legislation (e.g. covering electronic communications marketing). The Information Commissioner's Office (ICO) also publishes relevant guidance. The UK GDPR essentially mirrors the data protection regime that existed pre-Brexit.

Broadly, the UK GDPR protects the use of individuals' personal data. This is data from which an individual can be identified. Anyone who controls or processes personal data has to do so in accordance with stated principles (e.g. that they will do so lawfully, fairly and transparently, only for a specific purpose, only for so long as is necessary, only with appropriate technical or organisational security measures etc.) – and be able to demonstrate that they have done so.



Failure to comply with the UK GDPR can lead to severe penalties. In some circumstances, the ICO can impose fines up to the greater of £17.5m or (in the case of an undertaking) 4% of annual worldwide turnover. There are also related criminal offences.

Relevance for Pension Scheme Trustees

As pension scheme members provide trustees with a significant amount of personal data (e.g. name, address, date of birth, salary, bank account details, medical reports, etc.) trustees are obliged to ensure compliance with the UK GDPR. Although the UK GDPR can be difficult to apply to pension scheme situations, trustees will wish to be able to demonstrate compliance. One of the key challenges is the long term nature of pension schemes and how trustees ensure compliance with the principle to process personal data for no longer than is necessary (particularly as trustees have obligations to keep records, in some cases for six years, under pensions legislation and in any event may want to hold personal data longer than that).

Key practical steps – what does this mean in practice?

- conduct a data audit and impact assessment to identify what personal data is held by the scheme, who it is shared with and what security processes are in place;
- provide members and beneficiaries with a "fair processing" notice setting out the legal basis upon which the trustees controlled and processed personal data (giving data subjects this information is a requirement of the UK GDPR) – a key consideration for trustees is the basis upon which they control and process "special category data" (e.g. health or sexual orientation information) particularly of dependent beneficiaries (e.g. those named on an expression of wish form) as such persons do not, before the relevant member dies, have a direct relationship with the trustees and so cannot readily consent to the processing of their personal data;
- implement a data protection policy to set out how the trustees would comply with the GDPR (now UK GDPR) regime (including notification of breaches) and to demonstrate accountability for compliance (which is one of the data protection principles);
- review third party contracts with data processors (e.g. the scheme administrator) to ensure they are UK GDPR compliant;
- implement UK GDPR training for trustees - a key area is the requirement to notify the ICO/the data subject of a personal data breach in certain circumstances.

Many schemes will have considered these processes in 2018 but the obligation to ensure UK GDPR compliance is an ongoing one and trustee boards will wish to routinely consider UK GDPR compliance as part of their ongoing governance.

The Pensions Regulator has highlighted cyber security as a key concern for pension scheme trustees and at the time of writing this is a particular area where we are seeing trustee boards revisit and refresh their understanding.

Please contact us if you would like further information or advice on anything in this note.