Sackers

GDPR - one year on

Alert | 23 May 2019

Introduction

25 May 2018 was the dawn of a new era in the protection of personal data, with the GDPR building on and extending existing data protection provisions to create a regime "fit for the digital age". As the ICO said at the time, when it comes to compliance with the GDPR, "25 May is not the end. It is the beginning". So, as we reach the one-year mark, what should trustees (and employers) be doing to ensure continued compliance?

Key points

- Compliance with the GDPR and guidance issued by the Information Commissioner's Office ("the ICO") is an ongoing process.
- Whilst trustees have worked hard to update their systems, processes and contracts in line with the new legislation, now is the ideal time to take stock on what has already been done and what further action may be needed.
- The GDPR will continue to apply after Brexit, whether the UK exits with a deal or not, because the Data Protection Act 2018 ("DPA 2018") specifically incorporates the provisions of the GDPR into UK law.
- To help trustees and others, we have produced a series of Alerts and checklists on various elements of the GDPR requirements. These are available from the data protection area of our website.

Background

The GDPR raised the data protection stakes for all UK businesses (including trustees of occupational pension schemes) by introducing new obligations on both data controllers and processors.

As the ultimate responsibility for scheme personal data rests with them, trustees are data controllers for the purposes of the GDPR. As such, they are responsible for ensuring that any personal data is processed in a way that complies with relevant requirements. Failure to do so risks enforcement action (including prosecution) by the ICO and compensation claims from individuals.

Record keeping, contracts and demonstrating ongoing compliance

Audit / record keeping

As data controllers, trustees are required to keep a record of their personal data processing activities. The information gathered as part of their data audit exercise in the run-up to May 2018 can be used by trustees to help establish this. The record keeping requirements are ongoing and so records should be reviewed and kept up-to-date.

The ICO issued guidance on the requirements of Article 30 and "basic templates" to help data controllers and data processors document their processing activities, but this remains a complex area for schemes so legal input may be required.

Compliant contracts

Trustees, as data controllers, must have binding GDPR-compliant contracts in place with any data processor whose services they engage, such as the scheme administrator. Our checklist on governance and contractual requirements explains in more detail the steps trustees should take to document data sharing arrangements (see parts 4 and 5).

Finalising contracts should be a priority for trustees as unagreed terms pose certain risks, including potential sanctions from the ICO.

Training

As data controllers, trustees are responsible for, and must be able to demonstrate compliance with, the data protection principles. Trustees should consider undertaking appropriate refresher training as part of evidencing their ongoing compliance, which could include how these principles apply to the day-to-day running of the scheme.

Documenting the legal basis for processing

Trustees must determine the legal grounds they have for processing scheme personal data, bearing in mind that there will usually be more than one and they may change over time. Trustees must keep an ongoing record of the grounds on which they are relying, together with a justification as to why they apply.

Where data controllers are relying on "legitimate interests" (ie that the processing is necessary for the purposes of legitimate interests pursued by the trustees or third party, such as the effective running of the scheme), a "legitimate interests assessment" should be considered to help evidence compliance. The ICO published guidance on what elements should be covered as part of a legitimate interest assessment, and has issued a sample template which can be used for this purpose.

Policies and procedures

Data protection policy

Data protection policies should be reviewed at appropriate intervals and kept up-to-date.

Trustees should review and consider updating their policies in the light of experiences gained in the last 12 months. Our checklist on governance and contractual requirements explains in more detail what trustee data protection policies should include (see part 3).

Data subject access requests

Whilst the right to make a subject access request existed before 25 May 2018, it has gained traction since the GDPR came into force, with the volume of requests rising fast over recent months as awareness has grown.

With tight timeframes for responding, it is essential that trustees have a process in place for dealing with such requests. Key providers, such as scheme administrators, should also be under a contractual obligation to provide assistance here.

Personal data breaches

No matter how many carefully crafted policies, procedures and systems are in place to protect personal data, breaches can still happen, with information being inadvertently shared, accidentally damaged, lost or destroyed altogether. Depending on the level of risk posed to the individual, controllers may need to report the breach to the ICO (within 72 hours, where feasible), or to both the ICO and the individual concerned. The trustees will also need to record any potential breach.

It is therefore vital for trustees to have a process in place to deal with personal data breaches, ensuring that it works in practice, with key individuals made aware of their responsibilities.

Ongoing management of data protection issues

The need to manage data protection compliance and risks is ongoing. In addition, experience of dealing with data protection issues will evolve and the ICO will continue to issue and update guidance. Trustees should consider how to address ongoing compliance, and this should include deciding the frequency of reviews and documenting this in their scheme's business plan.

More recent developments

Cyber security

It is widely recognised that cyber risks pose a serious and ever-present threat to organisations reliant on their information technology systems and processes.

TPR has published guidance on "cyber security principles for pension schemes", which highlights the need for trustees to have processes in place to deal with cyber risks, and encourages them to actively engage with their advisers on this.

Processing special categories of personal data without consent

Subject to certain safeguards being met, the DPA 2018 permits the processing of special categories of personal data without consent "if the processing is necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on the controller or the data subject in connection with employment, social security or social protection…".

In our view, this easement can extend to trustees. So, if they have not done so already, they should discuss this with their legal advisers and, if applicable, should address this point in their data protection policy so that the appropriate safeguards are in place.

Brexit

The DPA 2018 has been designed to help the UK demonstrate that it can provide an adequate level of protection for transfers both to and from the European Economic Area (EEA), as the UK will become a "third

country" after Brexit (although there may be a transitional period).

However, some detail is yet to be ironed out, and so pension schemes should keep an eye on developments here.

Next steps

As dealing with data protection compliance and risks is an ongoing responsibility for trustees, it is important to ensure that data protection remains high on schemes' agendas. Trustees should review and update their processes and documentation in light of their experiences, and as "best practice" develops and security measures develop and improve.

If you have any questions on any of the above, please speak to your usual Sackers contact.

Sacker & Partners LLP
20 Gresham Street
London EC2V 7JE
T +44 (0)20 7329 6699
E enquiries@sackers.com
www.sackers.com