Data Protection Bill 2017

Alert | 22 September 2017

Introduction

The Data Protection Bill promised by the Department for Digital, Culture, Media & Sport (DDCMS) was introduced to the House of Lords on 13 September 2017. One of the main aims of the Bill is to make the UK's data protection laws "fit for the digital age in which an ever increasing amount of data is being processed".

Key points

- The Bill is designed to bring the provisions of the EU's General Data Protection Regulation (GDPR) into UK law, subject to certain amendments.
- One of the proposed UK specific modifications is the ability for occupational pension schemes to process sensitive personal data without consent where certain conditions are met.
- The Information Commissioner's remit is to be reinforced and expanded. Among other things, the ICO will be required to prepare a code of practice providing guidance on sharing personal data.

Overview

By implementing the GDPR directly into UK legislation, the Government aims to ensure the continued free flow of data across the EU – something which will be required for the UK's future trading relationships.

The DDCMS explains that, without the Bill, the GDPR would apply in the UK until the Brexit process has concluded, and so too would the Data Protection Act 1998 (DPA), "causing legal uncertainty and confusion for both individuals and organisations in applying the law".

As the Act, once in force, will apply before and after Brexit, it is a hybrid beast which attempts to both incorporate the GDPR's provisions into UK legislation and at the same time replicate and update the existing Data Protection Act 1998. As noted in the Explanatory Notes to the Bill, "to fully understand the Bill, it is necessary to read it alongside the definitions found in the GDPR". This need to read two substantial pieces of legislation side-by-side to get the full picture is perhaps one of the inevitable challenges of addressing data protection legislation in the context of Brexit.

Exemptions

The GDPR permits EU member states to make their own laws, providing exemptions, derogations, conditions and rules in relation to certain areas (such as the prevention, investigation, detection or prosecution of criminal offences), and also in relation to a number of specified processing activities.

The processing of employee data is one such area and the Bill provides that employers will be able to process sensitive personal data if they meet strict conditions. For example, the processing must be necessary to comply with employment law requirements, and the data controller has an appropriate policy document in place.

A specific easement is also proposed for occupational pensions, which is designed to allow sensitive personal data to be processed without consent where the processing:

- is necessary for the purposes of making a determination in connection with eligibility for, or benefits payable under, an occupational pension scheme
- is not carried out for the purposes of measures or decisions with respect to the data subject, and
- "can reasonably be carried out without the consent of the data subject".

For the latter test to be met, the data controller "cannot reasonably be expected" to obtain the data subject's consent and must not be aware of the data subject withholding consent.

The drafting of this provision is somewhat tortuous, but it could be intended to help deal with sensitive personal data which may be held incidentally in respect of potential beneficiaries (for example, on death benefit nomination forms) or other historic information such as decisions relating to past-ill health cases.

Enforcement and sanctions

The Bill sets out how the enforcement regime will work, broadly replicating existing provisions of the DPA.

In particular, it lays down the parameters for the ICO to demand information and assess compliance, and the process for taking action in cases of non-compliance. It also provides data subjects with a right to complain to the ICO, and a requirement for the ICO to consider and respond to their complaint.

The ICO will be able to impose higher fines than currently under the DPA. The Bill converts the GDPR's maximum penalties for non-compliance, so that the maximum fine for a breach by a data controller is the greater of 4% of global group turnover, or £17m (€20m under the GDPR).

Next steps

The Bill is in its early stages, with the next reading – a general debate in the House of Lords – due to take place on 10 October 2017.

The Bill will need to be in place before the GDPR comes into force on 25 May 2018 and before the deadline of 6 May 2018 for introducing the provisions of the EU's Law Enforcement Directive into UK law (aimed at law enforcement agencies, national security and the intelligence services). But despite the Bill stating that it will become the Data Protection Act 2017, it remains to be seen whether it will clear the Parliamentary process before the end of the year.

Whilst the exact timing for the Bill will be confirmed in due course, what is clear is that what is in the GDPR will form the core of UK data protection legislation. It therefore remains well worth taking steps to comply with the new legislation as it can take time to assess the data schemes hold, and to undertake compliance work

so that schemes are ready for the new data protection regime from 25 May 2018.

How we can help

We are producing a series of Alerts on the different elements of the GDPR in the countdown to May 2018. In addition, we have produced a checklist on "Assessing pension scheme data – the questions trustees need to ask" which is available via our website.

We can also help trustees prepare for the GDPR in a number of ways, including reviewing existing or new contracts, updating your data protection policy, reviewing procedures, and drafting member communications. For assistance with any of these, or any other GDPR query you may have, 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