Examining regulation and enforcement in the UK Data Protection Bill

27/09/2017

Information Law analysis: What will the UK Data Protection Bill (the Bill) mean in practice? Hannah Crowther, an associate at Bristows LLP, takes a closer look at the provisions relating to regulation and enforcement, contained in Part 5 and Part 6 of the Bill.

What is the background to Parts 5 and 6 of the Bill?

Part 5 of the Bill concerns the function and responsibilities of the Information Commissioner (usually referred to as the Information Commissioner’s Office or ‘ICO’). It corresponds to Article 58 of the General Data Protection Regulation, (EU) 2016/679 (GDPR), and provides some further detail on the powers granted to the ICO under the GDPR. The provisions largely duplicate the corresponding provisions of the current Data Protection Act 1998 (DPA 1998), eg requiring the ICO to engage in international co-operation and imposing an obligation of confidentiality on ICO staff. One of the more interesting provisions is the power given to the Secretary of State to create regulations requiring controllers (but not processors) to pay charges to the ICO—thereby answering the question as to how the ICO will be funded once it no longer has to maintain a register of controllers.

Part 6 of the Bill contains the enforcement powers of the ICO. The ICO is granted basic enforcement powers under the GDPR, but the Bill sets out in greater detail the conditions under which these may be exercised, the process, and safeguards for recipients (such as the right to appeal).

The ICO will continue to regulate and enforce data protection laws in the UK. What additional or amended powers does the Bill propose to give the Information Commissioner to help achieve this?

The ICO’s enforcement powers remain broadly similar to those under DPA 1998—at least in the way they are structured. It will continue to be able to issue information notices, assessment notices (ie compulsory audit), enforcement notices and monetary penalties. However, there are some fairly significant changes to the scope of these powers:

- the most significant change is that all of these powers can now be exercised against processors (in respect of their processor obligations in the GDPR)
- under DPA 1998, the ICO can only issue an assessment notice against a public authority. Going forward, however, in accordance with the GDPR, the ICO will have the right to audit any controller or processor in order to assess whether it is complying with data protection legislation
- there is no threshold of materiality to trigger a monetary penalty—it can be issued for any failure to comply (again, this is to reflect the enforcement regime in the GDPR). Currently, monetary penalties can only be issued where there has been a serious breach, which was likely to cause substantial damage or substantial distress, and where the controller acted either deliberately or negligently. However, it is worth noting the ICO’s recent comments that fines will continue to be a ‘last resort’, and so it is not expected that the ICO will begin issuing fines for minor violations
- of course, the most eye-catching aspect of the GDPR is the vastly increased fines which the ICO will now have at its disposal. The amount of €20m or €10m cap in pounds sterling will be calculated using the exchange rate of the day—alternatively, the fine can be up to 2% or 4% of global turnover (depending on the nature of the breach)

The Bill reproduces many of the criminal offences in DPA 1998, but some new offences are proposed. Which are the most significant new offences created or updates to existing offences?

The most significant new criminal offence in the Bill is that of knowingly or recklessly re-identifying information that is de-identified personal data without the consent of the controller responsible for de-identifying the personal data. The explanatory notes explain this was introduced to address concerns that have been raised (eg by the National Data Guardian for Health and Care) about the security of de-identified data in online files. This offence would be committed if, for example, an employee involved in medical research sought to discover the identities behind the pseudonymised patient data they were analysing. However it will be a defence if the person acted in the reasonable belief that they were, or had the consent of, the data subject/controller (or would have had it had the data subject/controller known).
The Bill also creates a new criminal offence of seeking to prevent the disclosure of information in response to a subject access request by altering, defacing, blocking, destroying or concealing the data.

**How will the proposals improve upon the enforcement regime for data protection breaches currently in place under DPA 1998?**

The possibility of turnover-based fines has already increased the significance given to data protection compliance by organisations across the UK. While very large fines are expected to be few and far between, there is no doubt that the threat of them (as well as the headlines they will generate) can help improve compliance.

Removing the requirement that the breach be likely to cause substantial damage or distress should also make life easier for the ICO. It would be possible to flagrantly breach many of the GDPR requirements, and even impact a very large number of individuals, but still fail to cause substantial damage or distress—it seems sensible that the ICO should still have the possibility to issue a fine in these circumstances.

**Are there any other points of interest worth mentioning here?**

There is an interesting point about the extra-territorial jurisdiction of the Bill, hidden away in clause 186(2). Although the territorial application of the Bill essentially mirrors Article 3 of the GDPR, the UK has taken an expansive approach in respect of processors without an establishment in the UK.

Under Article 3(1), the GDPR will apply to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the EU. The Bill applies this as meaning that it will apply to a processor in all cases where the controller is subject to the UK law, regardless of where the processor is established (and don’t forget the processor may in fact be a sub-processor, or even a sub-sub-processor). The safest thing, therefore, is for any organisation to assume that if they are handling data about UK data subjects, the UK law will apply. How this will be enforced in practice, where the organisation has no UK presence, remains to be seen.

_Hannah advises on a wide variety of data protection issues, ranging from enterprise-wide GDPR compliance projects and Binding Corporate Rules, to responding to individual subject access requests or complaints. Her practice includes a significant amount of contentious work, advising clients on managing data breaches and investigations by the UK Information Commissioner and other EU data protection authorities. She is also experienced in data protection litigation, assisting with cases before the UK Court of Appeal and the Court of Justice of the European Union._

*Interviewed by Kate Beaumont.*

The views expressed by our Legal Analysis interviewees are not necessarily those of the proprietor.

*This article was first published on Lexis®PSL Information Law on 27 September 2017.*

FREE TRIAL