BCLP. Client Intelligent

Insights

DATA PROTECTION REFORM – WILL THE UK SCORE ITS BURDEN-REDUCING GOALS?

Apr 11, 2023

On 8 March 2023, the newly-created Department for Science, Innovation and Technology ("**DSIT**") introduced the UK government's updated proposals for data protection reform in the shape of the Data Protection and Digital Information (No.2) Bill (the "Revised Bill"). The reform process had been put on hold last September when the government abruptly withdrew the first bill from parliament, giving rise to an expectation that more radical draft legislation would ensue. However, the introduction of the Revised Bill resumes this process and does not depart significantly from proposals set out in the initial bill.

Compared with some of the radical ideas in the 2021 public consultation exercise (Data: A new direction), the Revised Bill appears more "light trim" than fundamental post-Brexit pruning. Technology Secretary Michelle Donelan described it as providing a *"new common-sense led UK version of the EU's GDPR [that] will reduce costs and burdens to British businesses",* with the government predicting savings of more than £4 billion for the UK economy over the next 10 years.

This briefing summarises the impact of the proposed reforms for "data protection as usual" operations.

A (MAINLY) REDUCED COMPLIANCE BURDEN FOR SMES?

One of the chief incentives put forward for UK data protection reform was to lighten the compliance burden for businesses, especially SMEs. Certainly, some movement towards this goal can be seen in the proposals, though they do not appear ground-breaking. In any event, larger organisations with operations in both the EU and the UK could struggle to realise any significant burden reduction (for example, if they want to adopt a unified internal approach, they are likely to align with the more stringent of the two regulatory regimes).

The main changes are:

- **Goodbye DPO, hello SRI:** In situations where formerly a data protection officer **("DPO")** would be required, organisations will instead need to identify a "senior responsible individual" **("SRI")** who will oversee data protection compliance. The SRI also has the ability to delegate this

responsibility. This reflects the reality that many smaller businesses already outsource the DPO function as it can be difficult to find the depth of expertise in-house. SRIs need only be appointed by (i) public bodies, or (ii) controllers and processors that carry out processing of personal data that is likely to result in a high risk to the rights and freedoms of individuals. Guidance on the role/status of currently appointed DPOs will be an important adjunct to this proposal (the Revised Bill and the accompanying explanatory guidance do not cover this);

- **Assessment of High Risk Processing ("AHRP"?) not DPIA:** The existing comprehensive data protection impact assessments **("DPIAs")** requirement in Article 35 of the UK GDPR will be narrowed in scope. Controllers conducting "high risk" processing will, however, still need to conduct an assessment and include a summary of the (i) purposes of the processing, (ii) an assessment of whether the processing is necessary and the risks it poses to individuals, and (iii) a description of how the controller intends to mitigate any risks. The previously mandatory requirement to consult the ICO prior to conducting high risk processing has been made optional;

- **"ROPA-lite":** Controllers and processors need only maintain records of processing activity **("ROPAs")** where their processing of personal data *"is likely to result in a **high risk** to the rights and freedoms of individuals"*. ROPAs can also contain less information (when compared, for instance, to the ROPA template that is currently available via the ICO's website). The exemption linked to companies with fewer than 250 employees has been removed;

- **Resisting "vexatious" Data Subject Requests:** These rights of individuals (access, deletion, etc) have been restricted slightly, with controllers able to resist ***"vexatious or excessive"*** requests (formerly these had to be *"manifestly unfounded or excessive"*). Examples given of vexatious requests include those intended to cause distress, not made in good faith or that are an abuse of process. The controller can refuse such requests or charge a fee. There is additional clarity proposed around time limits for response times, which reflects current ICO practice and guidance;

- **No more UK representatives:** The requirement for overseas controllers within scope of the UK GDPR to appoint a representative in the UK is removed;

- **Complaints management process:** Data subjects have a new 'right' to complain to controllers about any UK GDPR breach relating to their data, with controllers required to acknowledge receipt within 30 days. This is additional to the existing data subject rights (e.g. of access) and therefore is an additional burden, in effect. Controllers are required to take steps to facilitate this complaints process, and without undue delay to take appropriate steps to respond. Controllers may be required to inform the Commissioner about the number of complaints received (if further regulations are passed). The Commissioner will also be entitled to refuse to act on a complaint received from an individual who has already complained to the controller, provided that the controller is still handling the complaint and it was made under 45 days ago.

This could have the effect of reducing the volume of complaints reaching the regulator but this appears to be at the expense of an additional "triage" step managed by the organisation subject to the complaint.

- **Cookies:** A relaxation of the consent requirement is proposed for certain types of cookies. Prior consent will no longer be required for cookies solely for statistical analysis, or that are security update- or functionality-related. It will still be necessary to provide notice and the ability to refuse them, so cookie banners will not disappear entirely. The scope of "essential" cookies is also extended to include a further range of cookies (e.g. necessary to prevent or detect fraud) meaning that, for such deployments, notice must be given to a user, but no opportunity to refuse the cookie need be offered.

The speed of progress of the Revised Bill towards new law is difficult to gauge at this point. At the time of writing, the Revised Bill is awaiting its second reading in the House of Commons – i.e. at a very early stage. The Revised Bill is over 200 pages long and is accompanied by a further 132 pages of explanatory notes. As well as data protection reform, it also covers reform of the Information Commissioner's Office and the Information Commissioner role. The Revised Bill also contains measures to promote the provision of digital identity verification services and smart data schemes to empower consumers to manage, compare and switch services efficiently. Other proposals are aimed at facilitating data flows to support certain public services and law enforcement.

After the wide-ranging and ambitious aims of the original consultation exercise, the proposals in the Revised Bill appear unremarkable, even allowing for adjustments made since the initial version of the bill. However, the world is a somewhat different place in 2023 compared with 2021. As well as some unforeseen geo-political and economic developments, there is the perpetual sword of Damocles of the EU's adequacy decision, which expires in June 2025 unless renewed by the European Commission. It follows, then, that the UK's approach to reforming its data protection laws should be a cautious one, in order to maintain balance - both nationally and internationally. That remains the case, even if this means data protection continues to be a significant element of regulatory compliance for organisations of all sizes.

RELATED PRACTICE AREAS

- Data Privacy & Security

MEET THE TEAM

Geraldine Scali

London

geraldine.scali@bclplaw.com
+44 (0) 20 3400 4483
