BCLP. Client Intelligent

Insights

UK DATA REFORMS – CAUTIOUS FIRST STEPS ALONG THE EU ADEQUACY "TIGHTROPE"

26 July 2022

SUMMARY

The UK government set out its detailed proposals for data protection reform on 18 July 2022 in the form of the Data Protection and Digital Information Bill. Compared with some of the radical ideas in the 2021 public consultation exercise (Data: A new direction), the Bill seems to be more of a light trim rather than fundamental post-Brexit pruning. Of course, the form of the final legislation will depend on the new administration's appetite for data protection reform - whether far-reaching or otherwise. The legislation is expected to be passed by spring 2023 at the earliest.

The Bill is over 180 pages long and is accompanied by a further 130 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 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. Further proposals are aimed at facilitating data flows to support certain public services and law enforcement.

What follows is a summary of the main changes to the data protection regime.

A (mainly) reduced compliance burden for SMEs

One of the professed incentives for UK data protection reform was to lighten the compliance burden for businesses, especially SMEs. Certainly, some movement can be seen here, though it does not appear ground-breaking. In any event, larger organisations with operations in the EU as well as the UK are unlikely to be able to benefit significantly.

The main changes are:

- **SRI not DPO:** Where formerly a data protection officer (DPO) was required, those organisations will instead need to identify a "senior responsible individual" (SRI) who will oversee data protection compliance, and also has the ability to delegate this responsibility. This reflects the

reality that many smaller businesses already outsource this function as it can be difficult to find the depth of expertise in-house. Guidance on the role/status of current DPOs will be an important adjunct to this proposal (the Bill does not cover this);

- **Assessment of High Risk Processing not DPIA:** The comprehensive data protection impact assessments (DPIAs) requirement is narrowed in scope. Controllers conducting "high risk" processing will still need to conduct an assessment and include a summary of the purposes of the processing; an assessment of whether the processing is necessary and the risks it poses to individuals; and 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":** Records of processing activity (ROPAs) can be less detailed for all and the exemption for companies with under 250 employees applies unless there is "high risk" processing. There will still be a need to assess whether proposed processing is "high risk" and further guidance will be needed from the ICO;

- **Non-vexatious Data Subject Requests:** These rights (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 in respect of time limits for response times, which is reflective of 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 processes:** 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.

Anonymisation and Automated Decision Making (ADM)

- **Anonymisation:** Some changes are proposed to the personal data definition (when an individual is "identifiable" or not) to help bolster the robustness and certainty of

anonymisation. As anonymous data is not within scope of the UK GDPR, the proposed change aims at drawing a brighter line between personal data (in scope of the UK GDPR) and information that can be considered to fall outside it and therefore could be available in an unrestricted way for research and analysis.

To assist businesses, the amendments give two circumstances where information will be treated as information relating to an identifiable individual (and therefore personal data). The first is where the controller or processor can themselves identify a living individual from the information they are processing, by using reasonable means, and the second is where the controller or processor knows or ought reasonably to know that as a result of their processing another person is likely to obtain the information (for example, somebody with whom the information is shared) and that other person could identify a living individual using reasonable means.

- **ADM:** A decision is defined as being based on "automated processing" if there is no meaningful human involvement in the taking of the decision. The proposals extend the circumstances under which automated processing (which includes profiling) can be used to take "significant decisions" (i.e. decisions producing legal or similarly significant effects for the data subject). Previously, the circumstances were limited to: (i) where necessary for entering into/performing a contract with the individual, (ii) where authorised by law or (iii) with the individual's explicit consent. At the same time, the Bill introduces minimum safeguards, including informing the individual and allowing them to make representations, contest the decision and obtain human intervention on the part of the controller. Tighter controls (similar to the previous position) remain in place regarding ADM involving special category data (e.g. relating to health).

- **Purpose limitation and further processing:** The reforms also broaden the ability of a controller to undertake further processing of personal data in certain circumstances, where this further processing is compatible with the original purpose. There is a new annex to the UK GDPR which sets out the conditions when personal data may be further processed.

International transfers

- **Data protection test**: Worthy of mention is the addition of a "data protection test" to which the Secretary of State must have regard when making regulations approving transfers to third countries aimed at ensuring the standard of protection is not materially lower than the UK's standard. The matters listed in the test codify the Schrems II case law and include respect for the rule of law and individuals' rights of redress. Organisations will also be expected "acting reasonably and proportionately" to consider whether the data protection test is met for the purposes of completing a transfer risk assessment (TRA) when using the UK's SCCs (standard contractual clauses for data transfers to recipients in third countries). This could suggest more

flexibility will emerge around the TRA process, and could partially ease the burden on controllers relying on SCCs for transferring data from the UK.

- There are no revolutionary proposals in this area. This is, however, probably the most difficult area for UK legislators to navigate, given the need to preserve EU-bestowed adequacy for the UK's data regime. Delegates from DCMS (the government department sponsoring the Bill) speaking at a National Data Strategy Forum in mid-July emphasised that there had been discussions with the European Commission and EU member states to check that the UK's package of measures did not jeopardise the adequacy decision. The importance of retaining the adequacy decision was alluded to in the Bill's impact assessment which estimated the economic impact that UK businesses would face if the country's adequacy status was withdrawn, namely between £190 million and £460 million in one-off data transfer agreement "contractual papering" costs and an annual cost of between £210 million and £410 million in lost export revenue.

Electronic Direct Marketing and Cookies

- **Fines and exemptions:** Maximum fines for breach of the Privacy and Electronic Communications Regulations (PECR) are increased to the UK GDPR level, being £17.5 million or 4% of global annual turnover. There are also some smaller changes to be aware of, such as the right for non-commercial entities (charities, political parties) to benefit from the "soft opt-in" exemption for email marketing (removing the need for prior consent to email marketing if certain conditions are met).

- **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.

- **Telecom companies** (public electronic telecommunication service and public communication network providers) are also under a new obligation to report suspicious activity relating to unlawful direct marketing to the Commissioner within 28 days, and will be subject to a £1,000 fixed penalty fine for failure to do so.

After the wide-ranging and ambitious aims of the consultation exercise, the scale of the proposals in the Bill appears unremarkable. To misquote Neil Armstrong, what appears on offer is "*One small step for UK data reform, one **small step** in easing the compliance burden in this area*". However, given the "tightrope" of the EU's adequacy decision that the UK continues to navigate, perhaps the lack of "giant leaps" is no bad thing.

RELATED CAPABILITIES

- Data Privacy & Security

MEET THE TEAM

Anna Blest

London

anna.blest@bclplaw.com
+44 (0) 20 3400 4475

This material is not comprehensive, is for informational purposes only, and is not legal advice. Your use or receipt of this material does not create an attorney-client relationship between us. If you require legal advice, you should consult an attorney regarding your particular circumstances. The choice of a lawyer is an important decision and should not be based solely upon advertisements. This material may be "Attorney Advertising" under the ethics and professional rules of certain jurisdictions. For advertising purposes, St. Louis, Missouri, is designated BCLP's principal office and Kathrine Dixon (kathrine.dixon@bclplaw.com) as the responsible attorney.

© 2025 Bryan Cave Leighton Paisner LLP.