NEWS BRIEF

Data protection reform: setting the course for a new direction

On 10 September 2021, the government launched a consultation outlining significant legislative proposals aimed at creating an "ambitious, pro-growth and innovation-friendly" data protection regime. At a time of increasing global data protection regulation, the UK's proposed reforms are conspicuous for appearing to buck the trend. The consultation reveals an intention to move away from prescriptive rules and guidance, and towards a focus on outcomes and making the UK "the world's most attractive data marketplace".

The benefits of reduced regulation are not expected to be felt evenly; the consultation notes that small and micro businesses will benefit proportionately more. The government sees the potential to realise a net direct monetised benefit to the economy of £1.04 billion over ten years.

The consultation is, in fact, the government's first step in delivering on mission 2 of its 2020 National Data Strategy, which noted that the UK's data regime should not be too burdensome for the average company.

Processing and legitimate interests

The consultation reports an over-reliance by organisations on consent as a lawful basis for processing, in part due to uncertainty among organisations as to when they can validly rely on the legitimate interests basis for processing. It proposes an exhaustive and limited list of activities for which "legitimate interests" could effectively be deemed, so that companies would not need to assess the balance between the legitimate interest being pursued and the impact on the rights of data subjects. The consultation suggests examples of what would be deemed to be legitimate interests, such as activities that are necessary to review an organisation's network or system security. In all other circumstances, including situations where children's data are processed, the current balancing test would continue to be a requirement.

Accountability framework

The consultation proposes removing a number of components of the accountability framework under the retained EU law version of the General Data Protection Regulation (*679/2016/EU*) (UK GDPR), including the requirements to appoint a data protection officer, conduct data protection impact assessments, and maintain records of processing activities. Companies would instead be required to implement a privacy management programme that is tailored and proportionate to their processing activities.

Small and micro businesses would be the clear beneficiaries of this proposal, and the consultation notes that a strong programme would, in practice, have many of the same features as the current legislation. The government recognises that this may create additional burdens for certain organisations as a result of the increased discretion over how to deliver compliance within the accountability framework, but it appears to be looking to the Information Commissioner's Office (ICO) to provide guidance and mentions the ICO's current Accountability Framework guidance favourably (*https://ico.org.uk/for-organisations/accountability-framework/*).

Personal data breach reporting

Noting that there has been a tendency towards over-reporting of personal data breaches under the UK GDPR, the consultation proposes that, instead of events being reportable unless the personal data breach is unlikely to result in a risk to data subjects, the test should instead be that organisations must report a breach unless the risk to data subjects is "not material". The ICO would be encouraged to publish guidance on the types of incidents that would meet this threshold. Accompanying this, a voluntary undertakings process could be implemented, to enable certain organisations to provide a remedial action plan to the ICO.

Subject access requests

In a move that will be welcomed by many organisations, the consultation invites views on introducing a costs ceiling for subject access requests, allowing organisations to stop processing a request when their costs exceed a certain limit, similar to the regime under the Freedom of Information Act 2000. Alternatively, the reintroduction of a nominal fee, as was previously applicable under the Data Protection Act 1998, is also raised for views.

Privacy regulations

The consultation floats the idea of bringing the Privacy and Electronic Communications Regulations 2003 (*SI 2426/2003*) enforcement regime in line with that under the UK GDPR. This would allow the ICO the ability to issue fines of up to £17.5 million or up to 4% of global turnover. Another proposal would see the soft opt-in for email and SMS marketing exception modified, extending it for the first time to non-commercial organisations including charities and political parties.

Cookies

There is considerable momentum behind the proposals to relax cookie consent requirements, with one option being to remove the need for consent for analytics cookies, which would bring the UK in line with France's approach. A second proposal would see organisations permitted to place cookies without consent for limited purposes, effectively creating a list of exempt cookies.

Contrary to some reports, however, cookie banners are likely to remain widespread, as third-party or privacy-intrusive cookies would seemingly remain subject to a consent requirement. The requirement to provide individuals with clear and comprehensive information about the use of cookies would also remain. Overall, documents accompanying the consultation estimate that these proposals would relieve 30% of businesses of the cookie opt-in consent requirement, with an estimated reduction in annual compliance costs of £15.8 million.

International transfers of personal data

To reduce barriers to international data flows, the government intends to make greater use of the ability to grant risk-based adequacy decisions in respect of third countries, or even groups of countries, regions and multilateral frameworks. For transfers to countries that are not deemed adequate, the UK GDPR may be amended to allow alternative transfer mechanisms to be introduced and, significantly, for organisations to identify their own alternative transfer mechanisms. These

proposals should be considered alongside the ICO's consultation on international transfers, which was launched on 11 August 2021 and provides an indication of the ICO's expectations when it comes to assessing risk in the context of international data transfers (*https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/ico-consultation-on-data-transferred-outside-of-the-uk/*).

Automated decision making

Article 22 of the UK GDPR currently provides that where individuals are subject to an automated decision that produces legal effects in relation to them, or similarly significantly affects them, they have the right to obtain human intervention. The consultation does not make proposals on this issue, but invites evidence on the need for legislative reform, noting that the need to provide human review may become unworkable in future as the use of automated decision-making technologies becomes more widespread, particularly in the context of artificial intelligence.

ICO reform

The proposals on the ICO focus on increasing oversight and alignment of the ICO with other regulators, such as Ofcom and the Financial Conduct Authority. In addition, the government intends to reserve the power, as it has with those regulators, to set strategic priorities to inform how the ICO sets its own regulatory priorities.

Simpler and clearer or additional complexity?

Some three years after the EU GDPR came into force, UK organisations are again facing significant regulatory change. For SMEs and businesses that handle modest volumes of personal data, and that may still be perplexed about what UK GDPR compliance means for them in practice, the proposed reforms are likely to be welcome. They may even be envied by similar organisations in the EU; a review by the European Commission in 2020 reported that the EU GDPR was challenging especially for SMEs (*https://ec.europa.eu/info/sites/default/files/1_en_act_part1_v6_1.pdf*).

For businesses that handle larger volumes, or more critical types, of personal data, a shift to an outcomes-focused privacy management programme could present new, different challenges: what should their privacy management programme entail? How will the ICO's approach to guidance and enforcement achieve certainty and flexibility as the UK seeks to leave behind the more prescriptive aspects of the GDPR-based regime? For multinational organisations, particularly those with parallel UK and EU operations, the reforms could create an additional dimension of complexity, rather than reducing it.

Kate Brimsted is the UK Data Privacy and Security Lead, and Tom Evans is a senior associate, at Bryan Cave Leighton Paisner LLP.

The consultation "Data: a new direction" is available at www.gov.uk/government/consultations/data-a-new-direction and closes for comments on 19 November 2021.