

June 22, 2022

UK Government Publishes Its Response on the Reform of the UK Data Protection Regime

On 17 June 2022, the UK government released its much anticipated response to the consultation on the reform of the UK data protection regime. As part of the UK's post-Brexit national data strategy, the consultation gathered responses on proposals aimed at reforming the UK's data protection regime to boost the UK economy. In its response, the UK government has signalled which of the proposals it will be proceeding with and are likely to appear in an upcoming Data Reform Bill.

Attorneys
[Rohan Massey](#)
[Christopher Foo](#)
[Edward Machin](#)

Overall, these reforms do not overhaul the existing UK data protection compliance regime, which is derived from EU legislation such as the General Data Protection Regulation and ePrivacy Directive. Instead, the proposals are incremental and largely modify obligations that organizations will be familiar with under the existing regime. As expected, these reforms are largely business-focused, with an overall aim of reducing compliance burdens faced by businesses of all sizes and facilitating the use (and re-use) of data for research.

1. Proposals to modify requirements derived from existing data protection legislation

Several proposals amend existing requirements in current data protection legislation; including tailoring such requirements to the size of the organization and/or the risks presented by their processing of personal data; changing mandatory requirements to voluntary compliance obligations; or modifying thresholds for compliance or introduce additional exceptions to current obligations. These include:

- Introducing a new requirement for organizations to implement “privacy management programmes”; such programmes are to be tailored to the size of organizations and the risks presented by their processing. Under “privacy management programmes”, existing requirements to designate a data protection officer (**DPO**), conduct data protection impact assessments (**DPIAs**) and maintain records of processing activities (**ROPAs**) are replaced by more flexible and tailored requirements, such as measures to appoint a suitable “senior responsible individual” responsible for the privacy management programme, implement “risk assessment tools” and maintain “personal data inventories”. Existing DPOs, DPIAs and ROPAs may remain in place and can continue to be used to demonstrate compliance.
- Replacing the mandatory requirement to consult the Information Commissioner’s Office (**ICO**) when an organization has identified a data processing activity which poses unmitigable high risks, to a voluntary consultation regime.
- Removing the need for websites to display cookie banners to UK residents and permit cookies and similar technologies to be placed on a user’s device without explicit consent for a wider range of purposes. The UK government has also stated its intention to move to an opt-out model of consent for cookies once ministers are content that users have access to technology that supports them to effectively manage their preferences on how their data is processed, except in cases where a website is likely to be accessed by children.
- Extending the soft opt-in for direct marketing to non-commercial organizations.
- Introducing qualified exceptions to the balancing test required when relying on legitimate interests as a basis of processing (i.e. where there are clear public interest reasons for the processing to occur).

- Modifying the threshold to allow organizations to refuse to respond to a data subject access request, from ‘manifestly unfounded or excessive’ requests to ‘vexatious or excessive’ requests, in line with the Freedom of Information regime.
- Introducing reforms to ensure data exporters can act “pragmatically and proportionally” when using alternative data transfer mechanisms (e.g. standard contractual clauses).

These proposals aim to reduce the burden on data controllers, and to a smaller extent data processors, when complying with data protection legislation. The business-friendly focus of these proposals has raised concerns that they may undermine the European Commission's (EC) UK adequacy decision, which currently permits the free flow of personal data from the EU to the UK (for more information, see our alert [here](#)). The UK government notes that EC adequacy decisions do not require an ‘adequate’ country to have the same rules as EU legislation, and maintains that the proposed reform of UK legislation is compatible with such decisions.

2. Proposals to promote research/innovation

Several proposals are also designed to boost research and innovation. These include:

- Clarifying what constitutes data processing for research purposes.
- Including a broader notion of consent as a legal basis for scientific research.
- Introducing a qualified exemption to the requirement to inform/recontact data subjects under Art. 13(3) of the UK GDPR when re-using personal data for research purposes.
- Clarifying how data may be re-used (e.g. the circumstances that constitute further processing, and the applicable legal basis for such processing).
- Clarifying that the standard required for data to be considered anonymous is to be relative to the circumstances at the time of processing.
- Recasting restrictions on automated decision-making as a right to safeguards rather than a general prohibition.

As anonymous data is not considered personal data and thus falls outside the scope of the GDPR, the proposal to qualify the standard of anonymous data may potentially unlock a substantial amount of data available to organizations to use for analytics, research and other processing operations. However, organizations should ensure that they have a relevant legal basis to anonymize personal data in the first instance, as the act of anonymization is a processing activity that would fall within the scope of the GDPR.

With regards to AI, the UK government has also stated that it will further consider how fairness will factor in a wider governance context and introduce a new exception to enable the processing of sensitive personal data for the purpose of monitoring and correcting bias in AI systems. The UK government has also reiterated its intention to publish a white paper on AI governance in line with its national data strategy, and in line with its previous stance, has stated its intention not to legislate separately for AI (in contrast to the EU’s upcoming AI Act).

3. Proposals to reform the Information Commissioner’s Office

The UK government also intends to reform the ICO, the body tasked with oversight of the UK’s data protection regime. Its proposals include:

- Refocusing of regulatory enforcement on the most serious threats rather than the high volume of low level complaints.
- Reforming of the complaints framework - data subjects must attempt to resolve their complaint directly with the relevant data controller before lodging a complaint with the ICO, and the ICO has discretion not to investigate certain types of complaints (including complaints where the data subject has not first attempted to resolve the issue with the relevant organisation).
- Extending the ICO's enforcement powers to commission technical reports and to compel witnesses to attend interviews.
- Increasing the maximum fine the ICO may issue under the Privacy and Electronic Communications Regulations from GBP 500,000 to GBP 17.5 million / 4% of global turnover (whichever is greater), in line with the UK GDPR and Data Protection Act 2018.
- Amending the statutory deadline for the ICO to issue a penalty following a notice of intent: in specific circumstances, the ICO will no longer be required to issue a penalty within 6 months of issuing a notice of intent.
- Introducing a requirement on the ICO to set out the anticipated timelines for the phases of an investigation to the relevant data controller at the beginning of an investigation.
- Empowering the ICO to take action for nuisance calls, based on the number of calls generated by an organization, and subject communications providers to a duty to report suspicious levels of traffic.

Certain proposals, such as the proposals to reform the complaints framework and set out investigation timelines, will be welcomed by organizations as they provide opportunities for the internal remediation of complaints and the reduction of uncertainty in the event of an investigation. The refocusing of regulatory enforcement on serious threats coincides with a [recent announcement](#) that the ICO will now be able to retain up to £7.5 million of the fines issued in any one financial year; the impact of such developments on enforcement remains to be seen.

Takeaways

As these proposals have yet to be translated into a statutory instrument there is no immediate action required to be taken. The UK government has also stated that almost all organizations that comply with the UK's current regime will be in compliance with the future regime, and that many businesses, as a matter of good practice, have already implemented the new requirements. This means that, for organizations operating mainly in the UK, the overall impact of the proposals (as they currently stand) is likely to be minimal; similarly, if organizations operating internationally across the UK and Europe continue to benchmark compliance against EU data protection law, the overall impact of the proposals should also be limited. Regardless, as these proposals are also likely to trigger formal and informal feedback, particularly from European authorities, who have not yet stated whether they agree with the UK's position on compliance, the possibility of additional changes cannot be ruled out. We are watching this space closely for updates.