UK government resumes proposed reform of UK data protection laws

MARCH 2023

UK government resumes proposed reform of UK data protection laws

On 8 March 2023, the UK government resumed its proposed reform of UK data protection laws with the introduction to Parliament of the Data Protection and Digital Information (No. 2) Bill, a replacement to its earlier reform bill.

The earlier version of the Bill was published in July 2022 (under prime minister Boris Johnson) but was then put on ice by the UK government following the appointment of Liz Truss as prime minister in order to allow time for ministers to re-examine the scope of proposed reforms.

In a speech given at the annual conference of the Conservative party in October 2022, the Science, Innovation and Technology Secretary, Michelle Donelan (who is responsible for guiding the Bill through Parliament), announced that the UK would be "replacing GDPR" with a "business and consumer-friendly, British data protection system."

Whilst talk of replacing GDPR may have sounded radical, the changes set out in the Data Protection and Digital Information (No. 2) Bill are not a wholesale rejection and replacement of GDPR but a series of targeted reforms to the existing framework. A number of these changes (if enacted) will be significant for businesses processing personal data that is subject to UK data protection law.

In her statement accompanying publication of the Bill, Michelle Donelan announced that the proposed new laws will "release British businesses from unnecessary red tape to unlock new discoveries, drive forward next generation technologies, create jobs and boost our economy." The data protection reforms can broadly be grouped into changes that are intended to provide greater certainty to organisations that process personal data by clarifying aspects of the existing framework, and changes that are intended to meet the government's pro-business agenda. The Bill proposes amendments in the following areas (click on the links for the relevant section):

This Law-Now article focuses on the reforms to UK data protection law (UK GDPR and the UK Data Protection Act 2018) and summarises the key changes for businesses that process personal data that is subject to UK data protection law.

Updated definition of personal data

The definition of personal data under UK data protection law includes information 'relating to' an identifiable individual, with an identifiable individual being someone who can be identified 'directly or indirectly'. It is proposed to update the definition to specify what is meant by 'directly or indirectly' and by information 'relating to' an identifiable individual. The proposals to some extent codify guidance that has already been issued by the Information Commissioner. Businesses that have to grapple with whether or not information constitutes personal data may welcome the greater clarity that the UK government says these changes intend to provide.

Legitimate interests

Many businesses rely on the 'legitimate interests' basis set out in Article 6(1)(f) of the UK GDPR as the legal basis for their processing of personal data. Under the planned reforms, Article 6 will be updated to include some examples of processing that *may* be considered as necessary for the purposes of a legitimate interest. This includes processing for direct marketing, intra-group transmissions of data (whether relating to clients, employees or other individuals) for administrative purposes, and processing to ensure security of network and information systems. Controllers will still have to ensure that the legitimate interests are not outweighed by the rights and interests of the applicable data subjects, but businesses will likely welcome the clarity that this provides. The proposed list of examples is non-exhaustive and it will be interesting to see whether the government is lobbied to add further examples to the list.

'Recognised legitimate interests'

The Bill proposes a new legal basis for processing – processing that is for a 'recognised legitimate interest'. Unlike the changes above, controllers processing data for a recognised legitimate interest will only need to ensure that their processing falls within one of the activities listed in a new Annex to the UK GDPR (i.e. they will not need to perform a balancing test to ensure that the proposed processing is not outweighed by the rights and interests of data subjects). The list includes processing that is necessary for detecting, investigating or preventing crime, which the Explanatory Notes published alongside the Bill say would cover economic crimes such as fraud, money-laundering or terrorist financing. This may be useful to businesses that carry out these types of checks on their customers or other counterparties.

The other activities currently listed are limited to processing in the areas of public interest; national security, public security and defence; emergencies; safeguarding vulnerable individuals; and democratic engagement. The Bill proposes that the Secretary of State will have the power to add new categories to the list of recognised legitimate interests by Statutory Instrument (SI).

Further processing

Under current rules, personal data may only be collected for specified purposes and not further processed in a manner that is incompatible with those purposes. The reforms propose including a set of criteria for controllers to take account of when deciding whether their intended new processing is compatible with the original purpose, and a list of conditions that would be considered compatible with the original purpose.

The set of criteria would essentially enshrine in law the current guidance from the Information Commissioner for such compatibility assessments. The list of conditions is intended to be pro-business by providing greater certainty as to what would be considered compatible. It includes processing necessary for a controller to comply with its obligations in law and for detecting, investigating or preventing crime (including fraud, money-laundering or terrorist financing, as above). The Bill proposes that the Secretary of State will have the power to add new categories by SI.

Scientific research, including for technological development

In another of the pro-business changes, the Bill would update the UK GDPR so that references to processing for "scientific research purposes" is deemed to include any research that can reasonably be described as scientific whether publicly *or privately* funded and whether carried out as a *commercial* or non-commercial activity. This would include processing for the purposes of technological development or demonstration (as long as those activities can reasonably be described as scientific). In some respects this may be viewed as not changing much because the UK GDPR does not currently limit scientific research to non-commercial endeavours or exclude technological research. However, the express references will provide confidence to businesses that they can rely on the exemptions in the UK GDPR given to processing for scientific research purposes when that is commercial and/or in a technological field.

Perhaps the more significant change is that, in conjunction with this, it is proposed to amend the definition of consent to enable controllers to obtain consent to an area of scientific research where it is not possible to identify fully the purposes for which the personal data is to be processed at the time of its collection. Currently, consent will only be valid if it is given for a specific purpose. This presents a hurdle to the conduct of research, which by its nature may change course within a general field of investigation. Under the Bill, consent will be deemed to be for a specific purpose where it falls within the new definition of consent for scientific research purposes.

International data transfers

The Explanatory Notes say that the Bill is intended to facilitate international trade by providing a clearer and more stable framework for international transfers of personal data. The government proposes to achieve this by:

— introducing a risk-based approach to data transfers so that businesses can use standard data transfer agreements to send data to a third country provided that, acting reasonably and proportionately, they consider the standard of data protection provided by those transfer agreements (and by any additional measures) would not be materially lower than the standard under UK data protection law, and

— changing the rules on adequacy so that international transfers of personal data to a third country may be approved by the Secretary of State if the standard of the data protection in the country is not 'materially lower' than the standard under UK data protection law. The current approach (and the approach under the EU GDPR) is that protection must be of an 'adequate level', which means an equivalent level of protection. This government proposal may be viewed as a lower threshold and opposed by privacy campaigners.

Many businesses that transfer personal data internationally will likely welcome any reforms that replace the complex current regime with a more simple and clear set of rules. These changes will, of course, only apply to transfers under UK GDPR. Businesses that also transfer EU personal data will still need to comply with the EU GDPR framework.

This change (along with some others) may raise concerns that the proposed divergence from the EU GDPR puts at risk the EU-UK adequacy decision and, if UK adequacy were lost, that the benefits of any changes under the Bill would be outweighed by the additional costs for businesses operating internationally.

Fewer records of processing

The Department for Science, Innovation and Technology (DSIT) believes that "the existing European version of GDPR takes a highly prescriptive, top-down approach to data protection regulation which can limit organisations' flexibility to manage risks and places disproportionate burdens on small businesses." Under the proposed reforms, controllers and processors will only be required to keep records of processing that is likely to result in a high risk to the rights and freedoms of individuals. This change may have little practical benefit for businesses that process personal data that is subject to UK and EU data protection laws and who will therefore need to keep processing records in compliance with EU GDPR (which requires records of any processing activities, subject to some limited exemptions).

No more DPIAs

Under current rules, controllers must carry out a data protection impact assessment (DPIA) before carrying out processing that is likely to result in a high risk to the rights and freedoms of the applicable data subjects. The Bill proposes to do away with DPIAs and replace them with an 'assessment' of high risk processing. The requirements for completing such an assessment appear intended to require less effort than for a DPIA but in practice this may amount to little more than a change in name.

A key difference is that under the new rules businesses would no longer have to consult with data subjects on the intended processing (where appropriate) and prior consultation with the Information Commissioner (where there is high-risk processing and measures cannot be taken to reduce the risk) would be optional rather than mandatory under the present rules. These changes may well cause some concern to privacy campaigners.

No more DPOs

Businesses will no longer be required to appoint data protection officers (DPOs). Instead, if they carry out high risk processing (or are a public body), they will need to designate a 'senior responsible individual' who is responsible for certain data protection compliance tasks (much the same as under the current law). In a change from the current rules for DPOs, the senior responsible individual must be a member of the senior management, rather than reporting to them. Unlike with DPOs, the senior responsible individual will not have to be someone that has any particular expertise or knowledge of data protection law (although in practice they are likely to need that in order to perform the tasks required of individuals in this role).

Data subject requests

The government wants to amend the exemption that businesses can use to charge a reasonable fee or refuse to respond to a request from a data subject to situations where a request is 'vexatious or excessive' (rather than 'manifestly unfounded or excessive' under the current law). This change is likely intended by the government to remove what it describes as 'red tape'. The Bill proposes that 'vexatious' would include requests that are intended to cause distress, are not made in good faith, or are an abuse of process. The reference to 'good faith' may come under scrutiny as to its (potentially broad) meaning. The inclusion of abuse of process will be relevant to businesses involved in disputes where access requests are made as a means for obtaining early disclosure of information.

Automated decision-making

In its statement accompanying publication of the Bill, the DSIT said that the UK's existing data protection laws "are complex and lack clarity" for solely automated decision-making and profiling "which makes it difficult for organisations to responsibly use these types of technologies." The changes proposed by the Bill are intended to provide businesses with "more confidence" when using automated decision-making.

Under the current law, automated decision-making is prohibited unless three use cases apply. The government proposes relaxing this regime so that businesses must ensure certain 'safeguards' are in place if a *significant* decision will be made solely using automated processing. A stricter regime will apply to making significant decisions based on processing of special category data, which will only be permitted if one of two specified conditions is met. These proposed changes may be welcomed by businesses that use or are intending to deploy technology for this purpose but may be met with scepticism from privacy campaigners as weakening individuals' right not to be subject to automated decision-making at a time when the use of technologies that enable this, such as AI, are becoming more prevalent.

No UK representatives

Businesses that are subject to UK GDPR but not established in the UK will no longer be required to appoint a UK-based representative. The UK government believes that controllers and processors should be left to decide how to most effectively communicate with UK stakeholders (such as data subjects and the Information Commissioner) in order to meet their legal requirements under UK GDPR.

Changes to the ICO

The Bill proposes to abolish the Information Commissioner's Office (ICO) and replace it with a new "Information Commission". The Information Commissioner (currently John Edwards) will become the chair of the new Information Commission, which will be made up of a board of executive and non-executive members. This is more than simply a name change. The Secretary of State will have powers in relation to the appointment of the board members and this is likely to be viewed by privacy campaigners as eroding the independence of the UK's data protection regulator.

More cookies without consent

The Bill also proposes changes to the Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR). Currently only 'strictly necessary' cookies can be deployed on users' devices without their consent. The government proposes expanding this to include cookies that are used for statistical purposes and to improve services or website use, the stated intention being "to reduce the number of consent pop-ups people see online." Businesses will still need to provide information about the cookies that are deployed and provide users with a means to opt-out, but the removal of a consent step is likely to be welcomed by many.

New notification obligation for telecoms and internet service providers

The government proposes introducing a requirement for telecoms and internet service providers to notify the Information Commissioner of any reasonable grounds the provider has for suspecting that a person is contravening or has contravened any of the direct marketing regulations under PECR. Failure to do this will result in a fixed monetary penalty of £1,000. The Information Commissioner will be required to publish guidance as to what constitutes 'reasonable grounds'.

Fines under PECR aligned with UK data protection law

The government has proposed bringing the enforcement regime under PECR in line with UK data protection law so that the Information Commissioner will be able to issue fines of up to £17.5 million or 4% of the total annual worldwide turnover in the preceding financial year, whichever is higher, for the most serious breaches.

Digital verification services and smart data schemes

In addition to the changes to UK data protection law, the Bill implements the government's strategy for digital verification services and smart data schemes. The proposals for digital verification services will establish a regulatory framework for the provision of digital verification services in the UK and enable public authorities to disclose personal information to trusted digital verification services providers for the purpose of identity and eligibility verification.

The proposals for smart data schemes are intended to improve data portability of consumer data between service providers (beyond the data portability regime set out in Article 20 of the UK GDPR). The government hopes that these reforms will create a more competitive marketplace for consumers and are an extension of the open banking scheme (which enables customers to share their bank and credit card transaction data securely with third parties who can provide them with applications and services).

Watch out for future Law-Now updates on digital verification services and smart data schemes.

Key contacts

Emma Burnett
Partner
T +44 20 7367 3565
E emma.burnett@cms-cmno.com

Daniel Gallagher
Senior Associate
T +44 20 7367 3418
E daniel.gallagher@cms-cmno.com