FRESHFIELDS

UK announces data reforms: what businesses need to know

25 October 2024

On 23 October 2024 the UK government introduced the Data (Use and Access) Bill to Parliament (the DUAB). The DUAB is a wide-ranging and significant reform package with implications for all businesses operating in the UK. While businesses that already comply with the current UK regime will generally only need to make minor adjustments, they should consider opportunities to leverage the greater flexibility afforded by the Bill.

Some of the DUAB's most noteworthy provisions include those to:

- enable the establishment of smart data schemes;
- reform the Information Commissioner's Office (ICO), including its name, structure, duties and powers;
- amend aspects of the UK's data protection and ePrivacy law regimes
- raise the maximum fines under and ePrivacy law (eg relating to direct marketing and use of cookies) to the same high levels as under the data protection regime;
- establish a framework for the provision of digital verification services in the UK;
- extend certain data sharing powers to improve public service delivery;
- require retention of information by providers of internet services in connection with investigations into child deaths, and the provision of information for research into online safety (amending the UK's Online Safety Act);
- permit recognition of certain overseas electronic signatures, electronic seals and other trust services;
- reform the information standards for health and adult social care in England and the way births and deaths are registered in England and Wales;
- facilitate the flow and use of personal data for law enforcement and national security purposes; and
- establish a register of underground assets.

This article explains the background to the DUAB and the new concept of smart data schemes. Given their relevance to almost all companies, it focuses primarily on the proposed reforms to the ICO and the UK's data protection and ePrivacy regimes, and their implications for businesses.

Background to the DUAB

The DUAB is the new (Labour) government's successor to the 'Data Protection and Digital Information Bill' (the DPDIB) proposed by the last (Conservative) government and variously debated and amended from July 2022. The DPDIB lapsed when Parliament was dissolved ahead of the UK general election in July 2024. The DUAB is similar to the DPDIB but has some important differences.

The UK's current data protection and e-Privacy regimes are largely based on the EU's 'GDPR' and e-Privacy laws. In 2021 the UK replaced the EU's GDPR with the UK GDPR, which broadly mirrored the key provisions of the EU's GDPR except for some minor amendments needed as result of Brexit.

Smart data schemes

The government's announcements emphasise that the DUAB will enable smart data schemes, to allow for the secure sharing of customer and business data (eg, data held by a financial services or energy provider) with customers and certain authorised third-parties (eg for switching, personalised market comparison and account management services). The government hopes those schemes – like the UK's existing and highly successful Open Banking Scheme – will benefit customers and the economy.

In relation to financial services, the DUAB also provides that the government may order the Financial Conduct Authority to make rules requiring financial services providers and certain other persons to use a prescribed interface, comply with prescribed interface standards or participate in prescribed interface arrangements, when providing or receiving customer data or business data.

These smart data reforms have been compared to the data sharing powers under the EU's Data Act. However, the relevant EU Data Act rules only apply to connected products, whereas the DUAB will give the UK government far broader powers to introduce smart data schemes across widespread parts of the economy.

The DUAB will provide powers to introduce the schemes, but it remains to be seen how they will be exercised in practice.

Key data protection and ePrivacy reforms

Less divergence from the EU

The data protection and ePrivacy reforms proposed by the DUAB are generally more limited that those proposed by the previous DPDIB, reducing divergence from the EU's GDPR regime. For example, unlike the DPDIB, the DUAB does not include proposals to:

- clarify the definition of 'personal data' subject to the UK GDPR;
- remove the requirement for data controllers or processors established outside the UK to appoint a representative in the UK;
- replace the obligations to appoint a data protection officer;
- amend record keeping obligations;
- allow data controllers to charge a fee or refuse to respond to subject requests in more circumstances;
- replace data protection impact assessments; or
- impose new obligations on providers of electronic communications networks to notify the new Information Commission if they have 'reasonable grounds' for suspecting someone is undertaking unlawful direct marketing.

However, the reforms in the DUAB are still significant.

ICO

The ICO currently regulates the UK's data protection and ePrivacy regime along with many other information laws.

The DUAB will replace the ICO with a new supervisory authority called the 'Information Commission' and also make various reforms to the regulator's organisation and duties. For example, the Information Commission will be required by law to have regard to promoting innovation and competition. It will also grant the Information Commission some new enforcement powers (eg, the right to require an organisation to produce a report or compel a person to attend an interview in connection with an investigation).

The Information Commission will be empowered to take longer than six months to issue a penalty notice following its notice of intent where necessary and provided it does so as soon as reasonably practicable. This will give more time than the ICO currently has to complete investigations, which could help strengthen enforcement (and prolong the process), especially in the more complex cases.

Data protection

Significant data protection reforms include proposals designed to:

- give individuals a statutory right to make complaints to the data controller and impose a statutory obligation on those controllers to put in place processes to facilitate complaints and respond to them within certain time frames;
- empower organisations to implement automated decision-making in additional scenarios; except for some changes to government powers, the DUAB's proposals are broadly the same as those in the previous DPDIB which we reported on here;
- allow a more 'risk-based' approach to international transfers of personal data, and therefore facilitate more transfers of personal data outside the UK. This includes:
    - introducing a revised set of criteria that the government will use to decide if the laws of a non-UK country are generally 'adequate' and therefore personal data can be sent to that country from the UK without additional safeguards; and
    - a new statutory test that will govern how organisations should undertake transfer risk assessments that must be completed by organisations before using commonly used safeguards to transfer personal data outside the UK (eg, ICO-approved data transfer agreements or binding corporate rules);
- assist organisations using personal data in connection with undertaking certain research, including by: (1) clarifying a way for controllers processing for scientific research purposes to obtain consents where it is not possible to fully identify the purposes for which the personal data is to be processed at the time of collection; and (2) clarifying that certain commercial research activities can benefit from the special rules regarding research in the data protection regime (some changes are also made to liberalise processing for statistical purposes);
- assist controllers in determining whether processing of personal data for a new purpose is compatible with the purpose limitation principle;
- authorise certain processing necessary for the purposes of responding to a request by US authorities made in accordance with the Agreement between the UK and US on Access to Electronic Data for the Purpose of Countering Serious Crime;

- change to the calculation of timeframes within which responses to data subject requests must be provided and clarification of the scope of searches the controller is obliged to undertake. These changes benefit controllers, including by specifying they may:
    - ‘stop the clock’ on the response time if they were unable to respond to a request without receiving further information or clarification from the person making the request (building on rights to ‘stop the clock’ the ICO has already granted in its guidance on data subject access requests);
    - limit searches in response to a data subject access request to what is ‘reasonable and proportionate’ (although ICO guidance already states unreasonable or disproportionate searches aren’t required);
- create a revised ‘disproportionate effort or impossibility’ exemption in relation to the requirement for information to be given to data subjects where the data was not collected directly from them – intended to clarify that the exemption applies to all processing and provide a non-exhaustive definition; and
- empower the government to make provision that certain descriptions of processing are ‘special category’ personal data and therefore subject to additional data protection obligations – a change not foreshadowed by the previous DPDIB.

ePrivacy

The UK’s ePrivacy regime, among other things, governs aspects of direct marketing and the use of cookies and other tracking technologies. Some key proposals include:

- reforms to rules relating to the restriction on storing information or accessing in the equipment of subscribers/users which impact the use of cookies and other tracking technologies, including:
    - expressly extending those rules to the collection and monitoring of information automatically emitted by the equipment or where storage or access is instigated;
    - exempting certain further cookies (and the like) from the general requirement to obtain consent provided an appropriate right to object and certain information is provided, such as various cookies for analytics or to record preferences of subscribers/ users; and
    - giving the government powers to vary exemptions to those restrictions in the future; and
- making breaches affecting direct marketing and the use of cookies subject to increased fines equivalent to those under the UK GDPR (ie up to the greater of £17,500,000 or 4% of an undertaking’s total annual worldwide turnover, compared with a maximum of £500,000 currently).

Personal data breaches impacting public electronic communications services

Providers of a public electronic communications service (ie entities which provide any service allowing members of the public to send electronic messages, including telecoms providers and internet service providers) are subject to a personal data breach notification regime under UK ePrivacy laws, which is distinct from that under the UK’s general data protection regime.

Those obligations currently include notifying the ICO of a personal data breach within 24 hours. In February 2023, the ICO announced some relaxation to how it would enforce that deadline. The DUAB will specify in law that the obligation is relaxed to require reporting of breaches to the Information

Commission without undue delay and, where feasible, not later than 72 hours after having becoming aware of it (plus an obligation to explain any failure to notify within the 72 hours).

Future reforms

The DUAB includes various wide powers for the Secretary of State to make subsequent reforms through secondary legislation.

Implications and next steps

Most of the proposed reforms introduce relatively limited changes as compared with the current UK or EU GDPR and ePrivacy regimes. Businesses that already comply with the current UK regime will generally only need to make minor adjustments.

The DUAB promises greater flexibility and divergence in certain areas (eg, automated-decision making, data processing in connection with research and international transfers).

The DUAB will introduce some new burdens on organisations and a need for them to consider how they should adapt their existing processes. For example, businesses will face potentially far higher fines for infringements of the ePrivacy regime, new enforcement powers and the requirement to put in place a process to facilitate data subjects raising complaints directly with them.

The UK government has made clear that it understands the importance of keeping the UK's designation by the EU as an 'adequate' jurisdiction, which allows most personal data to be transferred from the EU to the UK without the need to put in place additional safeguards. It remains to be seen whether the EU institutions object to the DUAB (eg over reforms to international transfer restriction or the ICO). The UK's adequacy decision could be revoked if the EU deems the UK's regime no longer adequate. While that seems unlikely, divergence from the EU's regime may also increase the odds of a successful challenge to the UK's adequacy status before the EU's Court of Justice. Fortunately, the DUAB's closer alignment with EU law, as compared with the previous DPDIB, reduces those risks.

The DUAB is still at the early stages of the Parliamentary process and a date for its second reading in the House of Lords has yet to be announced. However, given the government's strong majority in Parliament, UK data reform seems likely to finally happen. Businesses and other organisations should start considering how they may adapt to, and take advantage of, the new reforms.