The Data Use and Access Bill (Part 3) — comparing it with the DPDI Bill

Concluding a three part article series on the UK's new data protection law, Alison Llewellyn, Senior Knowledge Lawyer and Katie Hewson, Partner and Head of Data Protection, Stephenson Harwood, summarise the primary thematic differences between the DUA Bill and its most recent predecessor, the Data Protection and Digital Information Bill

On 23rd October 2024, the UK government introduced the Data (Use and Access) Bill (the 'DUA Bill') into Parliament. The DUA Bill contains an assortment of data-related provisions, including amendments to UK data protection law, provisions for new smart data schemes, private sector access to public sector data, digital ID verification services, changes to the Information Commissioner's Office's ('ICO's') powers and structure, and more.

In this article, the third in our series, we conclude our analysis of the provisions to be introduced by the DUA Bill and summarise the primary thematic differences between the DUA Bill and its most recent predecessor, the Data Protection and Digital Information Bill (the 'DPDI Bill').

Not just personal data

It is important to note that the DUA Bill is a wide-ranging piece of legislation and covers more than just reforms to data protection laws. As well as establishing a legal framework for smart data schemes to boost competition by facilitating consumer data portability and introducing digital ID verification services (see 'The Data Use and Access Bill (Part 2)', Volume 25, Issue 5), the DUA Bill also supports the enhancement of public services.

In particular, the DUA Bill introduces a data-enabled infrastructure initiative aimed at improving data-sharing through the creation of a statutory framework for the National Underground Asset Register ('NUAR'), which is a digital map of underground infrastructure. Currently a voluntary arrangement, the NUAR will make it mandatory for underground infrastructure owners (e.g. gas providers and telecoms operators) to register asset data (i.e. electricity cables, water gas and high-pressure fuel pipes and other underground pipes and cables). Failing to comply with the duty to upload the necessary information about underground assets into the NUAR will constitute an offence, with the asset owner being liable to pay compensation for its failure to do so.

These changes aim to streamline information sharing and enhance the efficiency and safety of buried infrastructure management across the UK. As surface level infrastructure such as high-rise buildings and new builds continue to develop throughout the UK, the NUAR will be vital in mitigating the risk that cables and pipes will be accidentally — or maliciously — damaged. As a result of these provisions, organisations should benefit from a more comprehensive view of assets, enabling them to know exactly where any underground asset is placed. However, there will undeniably be an increased burden on organisations to provide accurate data.

DPDI Bill background

Stepping back again to see the big picture, it isn't possible to properly analyse the DUA Bill without having some regard to the history of the DPDI Bill, which provides useful context to the development of the DUA Bill.

The DPDI Bill was first introduced during the 2022-23 parliamentary session as an attempt by the UK government to reform the UK's data protection framework and modernise its approach to data management. It was carried over to the 2023-24 session in a slightly different iteration before subsequently being re-introduced to Parliament on 8th March 2024 after various amendments.

As the Prime Minister at the time called for a UK General Election to be held on 4th July 2024, the DPDI Bill — along with other legislation that was not passed before the end of the period during which Parliament was being prorogued — did not progress any further. This came as a relief to those in the data protection community who were concerned that it would have lacked appropriate scrutiny had it been fast-tracked through Parliament during the 'wash-up' period. Parliament was dissolved on 24th May 2024, confirming the DPDI Bill's lack of progression.

(Continued on page 8)

(Continued from page 7)

The DUA Bill was introduced under Prime Minister Keir Starmer's new government in late 2024.

Current status of the DUA Bill

Much of the DUA Bill still bears a strong resemblance to the most recent version of the DPDI Bill. However, whilst the DPDI Bill and the DUA Bill share common goals, the DUA Bill has evolved with some divergences in scope and focus. Further, there are some notable absences in the DUA Bill.

As the DUA Bill has completed its passage through the House of Lords, it has undergone a number of further changes, including the removal of a proposed mechanism for the collective management of data rights; edits to automated decision-making processes; the addition of provisions relation to the protection of children's data; and direct marketing rules. It arrived at the 'Report' stage at the House of Commons on 7th May 2025 with yet more changes still being proposed, including to raise the age for processing personal data in the case of social networking services from 13 to 16.

"It is worth observing that a significant factor contributing to the delay in the DUA Bill becoming enshrined in law, initially expected by May 2025, has been the ongoing debate over the introduction of provisions concerning intellectual property rights and the ability of rights holders to opt out of data scraping for AI training purposes."

It is worth observing that a significant factor contributing to the delay in the DUA Bill becoming enshrined in law, initially expected by May 2025, has been the ongoing debate over the introduction of provisions concerning intellectual property rights and the ability of rights holders to opt out of data scraping for AI training purposes. Previously considered by the UK government in a now-abandoned AI copyright code of practice, the 'lack of AI-related protection' in relation to data scraping was specifically raised during the DUA Bill's Second Reading in the House of Lords. This led to new clauses regarding transparency and compliance with UK copyright law by operators of web crawlers and general-purpose AI models being introduced. These were voted against by the House of Commons, but concessions are now being considered for re-inclusion to assuage concerns, including from high profile creatives, about the impact of AI companies being able to use copyrighted works to train their models without permission, unless the copyright holder opts out of the process. These measures have proven highly contentious with a difficult balancing act to be made between the concerns, and a recognition that the quality of output produced by generative AI systems is largely dependent on the quality and quantity of data used for training them. It also shows the multi-faceted nature of the DUA Bill, which could be criticised for being a somewhat disparate patchwork of data-related and data-adjacent reforms.

The DUA Bill and UK adequacy

There is a strong likelihood that changes introduced by the DUA Bill have been heavily influenced by the government prioritising maintaining the UK's EU adequacy status for the purposes of conducting international data transfers. Developing international business is aligned with the UK government's agenda for growth, and possessing adequacy status is considered key to encourage international trade, given the legal certainty it gives over international personal data transfers to the UK. It is easy to see that diverging data protection frameworks risk bringing complexity and operational challenges, and UK lawmakers understandably want to avoid creating additional barriers to cross-border data transfers that could negatively impact international trade.

It is noteworthy that the European Commission's (the 'Commission') adequacy decisions in relation to the UK, published on 28th June 2021, were to remain in place until 27th June 2025, which is around the same time the DUA Bill was expected to come into force (in mid-2025, assuming no delays). However, the Commission proposed in March to extend its data adequacy decisions relating to the UK by six months, permitting continued free and secure data flows of personal data from the EU to the UK until 27th December 2025, allowing the Commission time to consider the DUA Bill and its contents in advance of making follow-up formal adequacy decisions.

The overall approach of the DPDI Bill versus the DUA Bill

You might be forgiven for still wondering what real changes were made to the abandoned DPDI Bill before it was resurrected as the DUA Bill. The DPDI Bill primarily sought to amend the UK GDPR and Data Protection Act 2018 (the 'DPA 2018') to reduce the compliance burden on businesses and encourage innovation. It notably proposed narrowing the definition of personal data and altering accountability obligations for organisations, such as replacing Data Protection Officers ('DPO') and easing data protection impact assessment ('DPIA') requirements. However, these have not been carried over into the DUA Bill.

While the DUA Bill is much broader in scope, it takes a more targeted approach to certain subject matters, for example, introducing a new focus on data mobility and smart data schemes, a new digital verification services framework, and amendments to data subject access requests ('DSARs'). The DUA Bill also avoids significant weakening of core GDPR

principles, reflecting concerns about EU adequacy and public trust in data governance.

Key retained sections from the DPDI Bill

Automated decision-making: A significant proposal in the DUA Bill that was preserved from the DPDI Bill is the dilution of the general prohibition on solely automated decision-making ('ADM'), where there is 'no meaningful human involvement', that produces legal or similarly significant effects.

Under the DUA Bill, ADM is generally permitted, provided that specific adequate safeguards are put in place. These include informing data subjects about such decisions; enabling their responses; providing for human intervention; and allowing decisions to be contested. Additionally, the Secretary of State may, by regulation, define which decisions have significant effects and modify or expand the associated safeguards. This reflects a more targeted and realistic regulatory approach that focuses on minimising risk rather than applying blanket restrictions.

The one area in which ADM continues to be prohibited (subject to exceptions) is for 'sensitive processing'. This is defined in relation to special category data and by reference to the DPA 2018 and includes, among other things, the processing of data concerning racial or ethnic origin, genetic data and health and it can only be fully based on ADM if the individual's explicit consent is provided, or the decision is authorised or required by law. These provisions aim to prevent misuse of sensitive personal information in high-risk contexts.

Narrowing the restrictions on the use of ADM may ultimately reduce protections for individuals, possibly necessitating the need for stricter regulatory oversight over the statutory safeguards to be implemented. It is clear that the softening of rules on ADM will facilitate the benefits of automation in a rapidly-developing AI landscape.

Recognised legitimate Interests: As in the DPDI Bill, the DUA Bill creates a new lawful basis for processing personal data under the UK GDPR: recognised legitimate interests. This includes a fixed list of purposes, such as responding to public interest requests; ensuring national security; managing emergencies; preventing crime; and safeguarding vulnerable individuals. These are now outlined in a new Annex 1 to the DUA Bill and modifiable by the Secretary of State through secondary legislation.

The effect of this amendment is that, in these specific scenarios, controllers no longer need to carry out a balancing test between their interests and the rights of the data subject. This removes a compliance hurdle and grants organisations greater certainty and operational efficiency when processing data in high-stakes contexts. For instance, in the case of emergencies, the Bill defers to the Civil Contingencies Act 2004, which lists qualifying disruptions such as terrorism or transport breakdowns. However, this shift raises important concerns. While the reform empowers organisations, it places a greater ethical and practical burden on them to ensure responsible data use — even without regulatory gatekeeping.

International data transfers: The DUA Bill mirrors the approach of the DPDI Bill as it establishes a new 'data protection test' that must be applied by the Secretary of State when deciding whether an international data transfer must be authorised and by organisations carrying out their own transfer impact assessments. This test creates a more flexible adequacy standard for third countries as it requires that their data protection frameworks offer safeguards that are 'not materially lower' than those of the UK.

However, the DUA Bill does not provide a specific definition of 'materially' in the context of the adequacy test for international data transfers. In practice, this means that a variety of countries may have different frameworks, both legal and cultural, that still arguably provide a sufficient level of protection for personal data. While this may broaden the pool of jurisdictions eligible for UK adequacy decisions, it could raise concerns for the Commission and potentially complicate the UK's adequacy assessment by the EU. From a practical perspective, organisations considering international data transfers might want to mitigate risk by seeking expert legal advice on whether and how local data protection laws comply with UK standards.

Charities direct marketing soft opt-in: The DUA Bill introduces a notable revision to the Privacy and Electronic Communications Regulations ('PECRs') by extending the soft opt-in for direct marketing to charities. This provision appeared in the DPDI Bill, before being dropped from the DUA Bill after the Labour government came into power, and then subsequently reintroduced in January 2025 during the DUA Bill's passage through the House of Lords.

Currently limited to commercial organisations, the amendment allows charities to send electronic direct marketing content to individuals who have donated or shown interest in their work, without requiring explicit prior consent, provided the charity offers a simple opt-out mechanism. This amendment aims to help charitable organisations communicate more effectively with their supporters, improving fundraising and engagement efforts, but is not without some controversy.

The amendment reflects a shift towards more flexible data use for public benefit but also places greater responsibility on charities to apply these rules transparently and proportionately.

Scientific research: The DUA Bill codifies a broad interpretation of 'scientific research'. This reduces the likelihood that the purpose limitation principle or restrictions on processing special category data will be an obstacle to research activities. The definition captures 'any research that can reasonably be described as scientific', regardless of whether it is publicly or privately funded, or conducted on a commercial or non-commercial basis.

(Continued on page 10)

(Continued from page 9)

As in the DPDI Bill, the DUA Bill sets out that references to scientific research include processing for technological development. However, by contrast, the definition of scientific research only applies when processing data for the purposes of a study around public health if the study can reasonably be described as being in the public interest.

This emphasises that while the aim of this change is undoubtedly to benefit research organisations, medical and health-related data still has additional safeguards protecting its use.

Cookies: Schedule 12 of the DUA Bill expands the scope of existing exemptions under the PECRs to permit the use of certain low-impact cookies and similar technologies without the need for prior user consent. This change aims to ease compliance for organisations while preserving transparency and user control.

The DUA Bill exempts from the requirement to obtain prior consent: functionality cookies that enable core features or support a website's display and usability; analytics/statistical cookies that collect usage data to inform website/service improvements; and personalisation cookies that recognise returning users and remember preferences.

Organisations must still provide users with clear, comprehensive information and a straightforward way to object to these cookies or similar technologies. The use of cookies for marketing purposes or any other use not covered by these exemptions will continue to require user consent under the PECRs.

Key differences between the DPDI Bill and the DUA Bill

Several proposed amendments from the DPDI Bill were not ultimately carried over to the DUA Bill. A number of these amendments fall under the accountability principle umbrella:

Maintaining a Record of Processing Activities ('RoPA'): Under the UK GDPR, all controllers and processors (unless exempt) are required to maintain a RoPA detailing their personal data processing activities and providing granular information covering the purposes of processing the data, the categories of data subjects and personal data, details of any transfers to third countries and any security measures taken concerning the data. An exemption to this was created under the DPDI Bill allowing organisations to be exempt from keeping a RoPA except in respect of 'high risk' processing. This modification to the UK GDPR was dropped from the DUA Bill, which still requires all controllers and processors to keep a RoPA, regardless of the type of data they hold.

Appointing a DPO: The DPDI Bill replaced the requirement for controllers and processers to have a DPO with a Senior Responsible Individual ('SRI'). Organisations can take comfort in the knowledge that the DUA Bill does away with the concept of an SRI altogether, leaving the DPO role unchanged.

Conducting DPIAs: The UK GDPR sets out a requirement to carry out a DPIA for high-risk processing. The DPDI Bill instead proposed that controllers should only carry out an 'assessment of high-risk processing', giving controllers more autonomy over the assessment method. The DUA Bil does not make any amendments to the current DPIA requirements.

Enhanced protections for children's data: The DPDI Bill lacked a comprehensive statutory basis for additional protections for children, merely giving the Secretary of State discretion to regulate that data can be processed because of a recognised legitimate interest to safeguard children's data, noting that children merit 'special protection with regard to their personal data'.

Changes to the DUA Bill to include further duties in respect of children's data were made during the House of Lords stage, including an additional duty on the ICO to have regard to the specific protections merited for children.

The DUA Bill introduces an amendment to Article 25 (data protection by design and default) of the UK GDPR, covering the processing of personal data when providing information society services likely to be accessed by children. In-scope controllers are mandated by the DUA Bill to take into account any 'higher protection matters' specific to the risks presented by processing children's data in their assessment of appropriate technical and organisational measures, which includes the fact that children have different needs at different ages and stages of development.

'Higher protection matters' in the DUA Bill are defined by reference to the fact that children are less aware of the risks and consequences of such data processing and of their rights in relation to such processing. An acknowledgement of children's possible lack of awareness around the use of their data is already present in Recital 38 of the UK GDPR, but enhancing statutory protections in the DUA Bill is a clear indication of the government's priorities.

Notably these 'higher protection matters' only apply to data protection by design, and not data protection by default. The difference between the two concepts lies in the fact that any data protection by design refers to proactive actions taken by organisations, as opposed to systems set to be automatically implemented i.e. by default to safeguard data protection principles and the rights of individuals.

The ICO has welcomed these changes but requested further clarity from the government on how organisations should actually interpret 'higher protection matters' in practice. Although the extent of the ICO's responsibility is yet to be fully defined, these requirements are in line with broader policy trends in the UK, most notably reflected in recent developments such as the Online Safety Act 2023 (which creates a duty of care for online platforms in relation to content that is harmful to children) and the Children's Code, an internet safety code of practice that draws from the GDPR and the DPA 2018.

Subject Access Requests: The DPDI proposed a potentially significant amendment to data subject access rights; conferring on controllers the right to refuse to respond to a data subject's request if it was 'vexatious or excessive'. This would be determined by several factors, including the nature of the request; the relationship between the data subject and the controller; and how long ago any previous request was made.

This amendment was ultimately omitted from the DUA Bill. While 'manifestly unfounded and excessive' requests may still be refused, this might appear to disadvantage organisations on the receiving end of DSARs compared with the DPDI Bill's proposals.

However, the DUA Bill balances this omission by retaining wording from the DPDI Bill in three ways. Firstly, in clause 78, it retains the DPDI Bill wording codifying the existing requirement established by regulatory guidance that any search should be 'reasonable and proportionate'. Secondly, any information to be provided does not necessarily have to be given if it would require a 'disproportionate effort', which depends on, among other things, the number of data subjects and the age of the personal data. Thirdly, the DUA Bill codifies the fact that controllers do not have to provide data subjects with information over which a duty of confidentiality is owed based on legal professional privilege.

While organisations would likely rejoice in the added ability to turn away frivolous DSARs, the DUA Bill is clearly trying to strike a balance between the burden on organisations and the rights of data subjects.

Special categories of personal data: The DUA Bill inserts a new provision into the UK GDPR allowing the Secretary of State, by secondary legislation, to define what types of processing of special category data are prohibited. The DUA Bill also inserts an equivalent provision into the DPA 2018 and further elucidates the concept of 'sensitive processing', allowing the Secretary of State discretion to designate certain personal data as sensitive. This term aligns with special category data processing under the UK GDPR, but is tailored for the national security context, potentially affecting how warrants are issued and reviewed.

The DUA Bill places more centralised control in the hands of ministers to regulate (or deregulate) sensitive data processing, raising potential balance of power and oversight considerations. Organisations processing health data, biometric data, or other special category data (for example in HR, marketing, or AI profiling contexts) must be aware that compliance obligations may shift quickly.

Conclusion

The DPDI Bill aimed to streamline the UK's data protection laws after Brexit by reducing administrative burdens for domestic businesses. The DUA Bill continues on this path, tempered by the recognition that if UK data protection legislation deviates excessively from the EU GDPR, this could threaten the UK's adequacy status, and ultimately stifle growth.

The DUA Bill both builds on and departs from the DPDI Bill, resulting in a revised — though not entirely novel — framework for data protection in the UK. Data protection laws in the UK will not fundamentally change, but organisations will need to be able to deftly navigate both additional and retained requirements from the DPDI Bill as the DUA Bill heads towards implementation.

As EU institutions are considering a reform of the EU GDPR, it will also be interesting to see how many of the UK's past and current proposals from both the DPDI Bill and the DUA Bill are considered for implementation in the EU.

The authors would like to thank Julia Benedict for her contributions to this article.

For information on PDP's training course, 'Data (Use & Access) Bill – Preparing for the Changes', see the website.

Alison Llewellyn and Katie Hewson
Stephenson Harwood
alison.llewellyn@stephensonharwood.com
katie.hewson@stephensonharwood.com