techUK

techUK.org | @techUK

Data (Use and Access) Bill

techUK briefing

The Data (Use and Access) Bill has the potential to strengthen the UK's data economy, all while maintaining robust protections.

The benefits of the UK's new data protection laws are ready to be seized ensuring data is a driver of economic growth. Data is a key enabler of economic growth, innovation, and more effective public services, with the OECD estimating that data access and sharing can generate social and economic benefits worth up to 4% of GDP when including both public and private sector data.

To fully harness these benefits, the UK needs a forward-looking regulatory framework that strikes the right balance between encouraging innovation and maintaining high standards of personal data protection. This balance is crucial for building trust in the new digital age.

techUK has been actively engaged throughout the development of the planned data reforms over the past three years, providing input through the Government's Business Advisory Group and other consultations. The Data (Use and Access) Bill presents an opportunity to create a clearer, more flexible, and more user-friendly to researchers and innovators data protection system while maintaining the UK's adequacy decision with the EU.

We would welcome the opportunity to meet with Parliamentarians to discuss the potential benefits of this legislation and how we can ensure that it delivers for the UK. For more information, or to arrange a meeting, please contact Audre Verseckaite at audre.verseckaite@techuk.org or Alice Campbell at alice.campbell@techuk.org,

Current challenges

Since its adoption in 2018, the UK's General Data Protection Regulation (GDPR) has presented certain challenges, with many organisations, regardless of size, citing a lack of certainty and clarity as holding them back from innovating with data, as well as significant regulatory burden. This briefing outlines the opportunities presented by the DUA Bill, while setting out specific areas where we advocate for further considerations and amendments. These include:

1) Making the UK a more attractive place for data driven research
2) Fostering innovation, competition and consumer choice by enabling Smart Data Schemes
3) Enhancing trust with Digital ID to support economic growth
4) "Recognised" legitimate interest list
5) Automated decision-making
6) A more flexible approach to international transfers
7) Researcher access to online safety data
8) Supporting pro-innovation regulation
9) Healthcare provisions – ensuring a unified, cohesive, and interoperable legislative framework for health and social care

The opportunity

Recognising current challenges and opportunities posed by data, the government has announced plans to reform the UK's data protection framework through the Data (Use and Access) Bill. These reforms aim to provide companies seeking to innovate with adequate access to high-quality research data, enable technologies that can increase user trust and facilitate the seamless flow of data within the UK economy. It will support the UK's ambition to become a global leader in trusted and responsible data-driven innovation and AI, giving businesses the confidence to invest in the UK.

1. **Making the UK a more attractive place for data-driven research**

We welcome the Bill's clarification of the existing UK GDPR provisions to explicitly state that commercial research can utilise data for R&D.

Historically, private sector organisations have underutilised these research provisions, due to risk-averse interpretation of the law. These changes will bring much needed clarity, particularly benefiting the development of cutting-edge technologies in fields such as artificial intelligence, healthcare, and environmental science. Combined with the recent expansion of the R&D tax credits to cover data and cloud computing, this will improve UK competitiveness as a destination for modern data driven R&D, helping increase the amount businesses invest here.

- While these changes clarify UK GDPR provisions, we are mindful that many companies also operate within the EEA, following GDPR rules. Therefore, the Government should work with the ICO to swiftly publish updated guidance on the use of personal data in research, and ensure that its publication aligns with the Bill's implementation schedule.

Examples of commercial R&D powered by data

Tackling financial exclusion: LexisNexis® Risk Solutions, part of RELX Group combined 2.6 million records with powerful statistical linking technology to provide a detailed, regional overview of financial exclusion and its underlying causes across the UK adult population.

Investigating emerging societal needs: BT's Global Research and Innovation Programme brought together BT's research ecosystem and was leveraged during the pandemic to explore growing concerns such as the future of work, impact on SMEs and in-person industries such as food, retail, and leisure.

Supporting medical research: Vodafone UK's DreamLab uses the processing power of mobile phones to accelerate scientific research. For cancer research, DreamLab has identified over 110 anti-cancer molecules and potential repurposed drugs, while for COVID-19 research, the app has employed AI to analyse virus-host interactome data, identifying potential antiviral treatments.

2. **Fostering innovation, competition and consumer choice by enabling Smart Data Schemes**

The Bill is expected to enable Smart Data Schemes in key sectors such as finance, transport, energy, and home buying, improving data interoperability and driving innovation. By fostering a more competitive and innovative market environment, the Schemes will support the growth of data-driven

businesses across the UK, providing consumers with greater access to diverse products and services. For example, Open Finance alone is estimated to have the potential to boost UK GDP by £30.5 billion annually.

3. Increasing trust through Digital ID to support economic growth

Trust is a critical driver of economic growth, with a 5% increase in digital trust potentially raising GDP per capita by over $3,000, according to the World Economic Forum. Trustworthy Digital IDs are a key enabler of this growth. In 2023, the UK Government estimated that widespread adoption could add £800 million annually to the UK economy through improved financial inclusion, reduced levels of fraud, and streamlined access to services like banking, public services, and retail experiences.

This legislation introduces important measures that aim to help underpin trust in Digital ID's, foster greater innovation, and encourage adoption, including:

- The requirement for the Secretary of State to publish a Digital Verification Service (DVS) trust framework document (the "trust framework"), which will set out baseline rules concerning the provision of DVS, and the power for the SoS to publish supplementary rules

- Establishing a public register of digital ID providers that have been certified against the trust framework and supplementary codes. As part of this process, this legislation grants powers to the SoS to refuse applications or remove providers from the register. The governance of the register will be managed by Office for Digtial Identities and Attributes (OfDIA) under the SoS, including assessing applications and removing providers from the register

- Enabling the SoS to designate a trust mark to be displayed by registered providers to distinguish their services in the market

- The Bill also enables information sharing between public authorities and registered providers, with consent, to support identity and eligibility checks.

In combination with Smart Data Schemes, these initiatives will be crucial in enabling the secure exchange of data between the public sector bodies, and between the public and private sector.

- ***Further areas for improvement and consideration:*** techUK continues to advocate for an independent regulator. While we continue to believe this is needed for a trustworthy digital ID market, working within the constraints of the Bill, we propose the Bill should be amended to create a structure that better reflects good governance practices. This could be achieved by establishing a clear process for market investigation, adjudication and appeals, whereby there is independent scrutiny of decisions related to the removal of providers from the DVS register, complemented by a well-defined right of appeal. We have included a list of proposed amendments aimed at enhancing the independence of the framework in the Annex A.

- It will also be important to ensure sufficient interoperability to fully realise the benefits of digital ID. Therefore, the government should prioritise making One Login interoperable with the trust framework, and with international standards. An example of One Login aligning to the trust framework could be for One Login to adopt the GPG45 model of levels of confidence/assurance, rather than the current 'vectors of trust' model they use.

4. Introducing a "recognised" legitimate interest list

The Bill introduces a list of "recognised" legitimate interests for data processing, encompassing public interest purposes such as national security, emergency response, crime prevention (including economic crimes like fraud) and safeguarding children or vulnerable adults. Previously, processing data for these purposes often required completing a lengthy balancing test. By explicitly recognising these specific public interest use cases, the Bill provides organisations with greater clarity and confidence in their data processing activities. This change also helps reduce compliance burdens, particularly when organisations are responding to urgent or serious situations.

Overall, techUK supports the approach to legitimate interests outlined in the Bill. In our view, it reinforces and clarifies what was already implicit in the existing GDPR framework, offering a more pragmatic solution for organisations handling sensitive or time-critical data processing.

- ***Further areas for improvement and consideration:*** However, the government should also consider expanding the recognised list to address other critical data processing needs, such as data processing for bias mitigation in algorithmic or AI systems. Clearer provisions would ensure organisations have clear legal grounds to tackle algorithmic bias effectively, helping enhance fairness while fostering public confidence in these emerging technologies.

5. Allowing for more automated decision-making in low-risk scenarios

The Bill will empower organisations to implement automated decision making (ADM) in low-risk scenarios – which make up the majority of ADM uses – such as service personalisation, faster logins, or estimating whether someone would be successful in a credit application. At the same time, it will set clear safeguards for the use of ADM in situations that could have legal or similarly significant effects on individuals, such as mortgage reviews, or employment decisions. This balanced approach includes the right for individuals to contest and seek human intervention on these decisions.

When combined with other provisions of the DUA Bill, such as legitimate interest, ADM can create significant societal benefits. For example, it could be used when analysing large amounts of data, including transaction history, device information, and customer behavior, to identify patterns that are indicative of fraud and help identify suspicious transactions before they are processed. This could significantly bolster the government's anti-fraud strategy by enabling organisations to proactively identify and address fraudulent activities, protect consumers, and safeguard the integrity of the wider economy. This underscores the importance of incorporating ADM into the broader regulatory framework to ensure its responsible and ethical use.

However, we also recognise the closely connected risks of AI technologies in amplifying existing inequalities and the role that a right to human review must play in significant decisions. This is essential to ensure that individuals have confidence that rigorous balancing tests are being conducted when decisions with significant or legal consequences are being made.

6. A more flexible approach to international data transfers

The DUA Bill reforms will ensure a more flexible, proportionate and risk-based approach to adequacy assessments and data transfer mechanisms. The Bill will also grant the UK government flexibility to adopt a broader range of safeguards for global transfers. These reforms align with the UK's ambition to become a global centre for data-driven innovation, addressing the growing complexity of the global landscape for international data flows and enabling the UK to respond effectively to emerging challenges.

techUK has noted suggestions from some stakeholders to amend the Bill and prevent any data flows to a range of countries on the basis of ability to seek remediation in those countries. However, we are of the view that the current Bill's provisions, as drafted, are preferrable. Otherwise, there may be a risk of significant harm to the UK by making it difficult or near impossible for data to flow from the UK to certain countries, which could have catastrophic impacts on trade in goods and services with potentially significant markets. Any proposals that would require the re-examination of existing adequacy arrangements could significantly impact any industry working with jurisdictions lacking adequacy agreements, disrupting essential business operations and international trade relationships. Furthermore, resourcing a regime which applied this would be particularly burdensome on the Government and the ICO.

The DPA 2018 already provides comprehensive frameworks for international transfers, with sections 17A and 17B setting out detailed factors for adequacy decisions. These existing mechanisms effectively address cross-border enforcement and remediation. The ICO's current role, established through an MOU with government, appropriately balances oversight with practical implementation.

- ***Further areas for improvement and consideration:*** Additionally, the Bill could provide additional flexibility for international data transfers by, for example, exempting "reverse transfers" from data transfer rules in the instances where data is already protected in its originating country, ensuring strong data protection is maintained.

Further areas for improvement and clarification

7. Researcher access to online safety data

Clause 123 (Information for research about online safety matters) introduces provisions for researchers to access online safety data from digital services. While we support the principle of enabling research access, the framework needs careful consideration to protect both user privacy and to ensure that sensitive company information is handled with care.

The current provisions outline the application process for data access and include privacy safeguards, requiring government consultation with bodies like Ofcom before implementing new rules. However, we believe the provisions need further refinement, particularly around the definition of qualified researchers (see Annex B for a proposed probing amendment).

techUK would urge a discussion between the Government and the private sector on this topic, which we would be happy to facilitate. This would help to ensure that this provision has the right definition.

8. Supporting pro-innovation regulation

techUK welcomes the government's continued focus on innovation-friendly regulation, reflected in both the Mansion House speech which introduced the concept of "regulation for growth," and the DUA Bill's requirement for the ICO to consider innovation and competition. These reforms align with broader efforts to make the UK a competitive hub for data-driven growth.

However, we are disappointed about the removal of provisions that would have supported regulatory alignment with broader policy objectives – namely, the requirement for the Secretary of State to designate a statement of strategic priorities for the ICO; as well as the ability to provide non-binding recommendations on the ICO's codes.

Similar frameworks operate effectively across other regulators without compromising their autonomy. Implementing these mechanisms would have aligned the ICO with established UK

regulatory practices, whilst maintaining its independence and strong data protection framework. They would have supported the government's "regulation for growth" vision by providing clear guiding principles for the ICO's powers. These changes would have brought greater predictability through improved transparency, an emphasis on guidance over enforcement, risk-based oversight, and innovative approaches to legal certainty, such as codes and certifications.

We are of the view that reinstating the requirement for the Secretary of State to designate a statement of strategic priorities for the ICO; as well as the ability to provide non-binding recommendations on the ICO's codes would provide much-needed additional oversight to the ICO. However, if this is not feasible, we propose two alternative approaches to strengthen the checks and balances within the ICO:

- ***Further areas for improvement and consideration:*** amending the Bill to ensure the ICO's non-executive membership – given their important oversight role – reflects a broader range of expertise in areas, such as civil liberties and freedom of expression, public administration, international trade, business and economics, consumer rights, and children's rights. This balanced composition would help ensure the Commission's strategic direction is informed by expertise beyond data protection, supporting the broader objectives of innovation-friendly regulation whilst maintaining robust protections (proposed amendment set out in Annex C).

- Additionally, the ICO's regular multi-year strategy should be specifically required to address how the regulator intends to deliver a balance between a risk-based approach to the protection of personal data, and ensuring that it supports safe, responsible innovation with data. This could provide a metric against which parliamentarians and the ICO's non-executive board could measure success.

9. Healthcare provisions – ensuring a unified, cohesive, and interoperable legislative framework for health and social care

The health and social care sector has seen a proliferation of disparate legislative frameworks and at times conflicting guidance, which has created a complex and fragmented landscape. This has led to inconsistencies in data retention practices, hindering interoperability and posing challenges for suppliers operating under diverse contracts. These concerns have been recently echoed in the Sudlow Review, which specifically highlighted the need to streamline processes and reduce unwarranted complexity in the health data landscape.

Schedule 15 of the DUA Bill will amend the Health and Social Care Act 2012 (HSCA 2012), aiming to establish a more comprehensive framework for information standards in health and adult social care. It clarifies that the information standards apply to information technology (IT) and IT services and extends their scope to public bodies that have roles related to health care and adult social care. The Bill also outlines enforcement mechanisms and paves way for an IT accreditation scheme.

techUK supports the intention behind the proposed legislation for health and social care and recognises its potential to introduce greater consistency and standardization within the sector.

However, to fully realise this potential, it is crucial that the new legislation and guidance are seamlessly integrated into the existing frameworks. This will minimise the risk of conflicts and ensure a truly cohesive approach.

To achieve this, we would urge the government to take a comprehensive approach to legislation and guidance, ensuring seamless alignment across all regulations, minimising potential conflicts. In addition, the government should issue clear and consistent guidance on how to resolve conflicts between different legislative frameworks, empowering stakeholders to navigate these complexities effectively.

Finally, close engagement between NHS England, DHSC, DSIT, and the health and care technology industry is essential to help to ensure that the changes resulting from the Bill ultimately improve outcomes for patients and staff and help build a vibrant health-tech industry in the UK. As DHSC considers the recommendations from the Sudlow Review, this presents a good moment to align the implementation of the DUA Bill with broader efforts to streamline the health data landscape.

We would also welcome more insight from the Government on how these specific measures will be enforced in practice.

Annex – proposed amendments

Annex A – Digital Verification Services

These amendments were discussed in the House of Lords during Committee Stage on 3 December 2024 and were not passed.

Clause 28 Digital Verification Services Trust Framework

(1) The Secretary of State must prepare and publish a document ("the DVS trust framework") setting out rules concerning the provision of digital verification services.

(2) Those rules may include (among other things) rules relating to, and to the conduct of, a person who provides such services; and references in this Part to a person providing services in accordance with the DVS trust framework (however expressed) include a person complying with such rules. Those rules must include processes for ongoing monitoring of compliance, including but not limited to processes and procedures for monitoring and investigating compliance. The rules must contain mechanisms for redress for harms caused by compliance failures. The Secretary of State must establish an independent process for hearing appeals against the findings of compliance investigations.

(5) The Secretary of State must publish a 5 year strategy for digital verification services in the UK, following written consultation. This strategy will establish key performance indicators. The Secretary of State must report progress to Parliament against those performance indicators annually. The Secretary of State may revise and republish the DVS trust framework (whether following a review under section 31 or otherwise).

Clause 31 Review of DVS trust framework and supplementary codes

(1) At least every 12 months, the Secretary of State must— (a) carry out a review of the DVS trust framework, including but not only for performance against the 5 year strategy and associated performance indicators, as well as the effectiveness of compliance monitoring and investigations activities, and (b) at the same time, carry out a review of each supplementary code which has not been withdrawn.

Clause 34 Power to refuse registration in the DVS register

(1) The Secretary of State may refuse to register a person providing digital verification services in the DVS register if the Secretary of State— (a) considers that it is necessary to do so in the interests of national security, or (b) following the completion of established investigatory processes and independent appeal is satisfied that the person is failing to comply with the DVS trust framework in respect of one or more of the digital verification services in respect of which the person applies to be registered.

Clause 34 Power to refuse registration in the DVS register

3(d) The notice must— (a) state the name and address of the person, (b) state the reason why the Secretary of State— (i) considers that it is necessary to refuse to register the person in the interests of national security, or (ii) is satisfied that the person is failing as mentioned in subsection (1)(b), (c) state whether the Secretary of State intends to specify a period in the notice under subsection (8) and, if so, what period is intended to be specified, (d) state that the person may make written representations to the ~~Secretary of State~~ independent appeal body about— (i) the Secretary of State's intention to refuse to register the person in the DVS register, and (ii) 35 where relevant, the period the Secretary of State intends to specify in the notice under subsection (8), and (e) specify the period within which such representations may be made. Representations may be made in line with the rules established for monitoring and investigating compliance with the trust framework.

Clause 40 Duty to remove person from the DVS register

(1) The Secretary of State must remove a person from the DVS register if the person— (a) has caused failure to comply with the trust framework such that the independent appeals body recommends removal; (~~ab~~) asks to be removed from the register, (~~bc~~) ceases to provide all of the digital verification services in respect of which the person is registered in the register, or (~~cd~~) no longer holds a certificate from an accredited conformity assessment body certifying that at least one of those digital verification services is provided in accordance with the DVS trust framework.

Clause 41 Power to remove person from the DVS register

(1a) The Secretary of State may remove a person from the DVS register if— (a) following the conclusion of an investigation process the Secretary of State is satisfied that the person is failing to comply with the DVS trust framework when providing one or more of the digital verification services in respect of which the person is registered,

Annex B – definition of researcher

Clause 123 - Information for research about online safety matters
Page 153, after line 10, insert -
"( ) the definition of "independent researcher,"

Explanatory note: To enable the Secretary of State to make provisions about the definition of researchers.

Annex C – make up of ICO's non-executive membership

Schedule 14

Page 232, line, after line 8 insert -

"*Membership: non-executive members expertise*

4A In making recommendations of persons for appointment as non-executive members, the Secretary of State must ensure that the membership of the Commission includes non-executive members with expertise in:
(1) Civil liberties and Freedom of Expression,
(2) Public Administration,
(3) International Trade,
(4) Business and Economics,
(5) Consumer Rights, and
(6) Children's Rights."

Explanatory note: To ensure that non-executive members of the Commission have a sufficient balance of expertise to inform the Commission outside of purely data protection issues.