techUK

techUK.org | @techUK

Data Protection and Digital Information (No. 2) Bill

Briefing for MPs and Lords

techUK sets out our key positions about the Data Protection and Digital Information (DPDI) (No. 2) Bill and outlines key areas where we would like to see further amendments.

Introduction:

Following withdrawal from the European Union (EU) there is an opportunity for the UK to develop a tailored data protection regime that works better for British society and businesses, prepares us to seize the benefits of AI technologies, while also maintaining a globally recognised high standard of data protection rights and preserving data flows with our international partners including the EU.

The reforms will make the UK's data protection system clearer, more flexible, and more user friendly to researchers, innovators, and smaller companies. It will also empower consumers through the establishment of the Digital ID Trust Framework, which will spur on the use of digital identities, enhancing security, streamlining authentication processes, and providing convenient and efficient access to various online services.

Building on the GDPR:

Since its adoption in 2018, the UK's General Data Protection Regulation (GDPR) has had limitations, with many organisations, regardless of size, have citing a lack of certainty and clarity as holding them back from innovating with data. Smaller firms, in particular, find it more difficult to absorb the more onerous compliance requirements of the existing regime.

With the EU also set to review its GDPR, the UK is in a unique position to be a global leader on future data governance by building on a global standard of data protection to make it better suited for our modern digital economy. Achieving this means making changes, but also upholding the key principles of the GDPR which the UK was instrumental in creating while part of the EU.

This briefing outlines the opportunities presented by the DPDI Bill, such as leveraging data to address the UK's challenges and safeguarding the data rights of consumers. Additionally, it also sets out specific areas where we advocate for further amendments. These are:

1. Making the UK a more attractive place for data driven research
2. Ensuring the recognised list of legitimate interests works as intended
3. A more flexible approach to International transfers
4. Allowing the UK's Digital ID market to grow
5. Maintaining EU Adequacy
6. Addressing concerns over the Secretary of State's Powers

7. Automated telephone marketing – technical feasibility of new obligations to report on nuisance communications

8. Ensuring a unified, cohesive, and interoperable legislative framework for health and social care

The Opportunity: enabling data to be used to solve the UK's challenges

The Bill will amend the UK GDPR in ways that support the use of data to solve some of the UK's most pressing challenges from providing clearer bases for using data in research in development to giving companies more certainty to process data to prevent crime, respond to emergencies and to safeguard children or vulnerable adults.

This will be done by clarifying areas of the regime, introducing a focused list for the legitimate use of data, and applying a more proportional and risk-based approach for SMEs and small organisations.

To ensure the Bill is successful at addressing these challenges, we are of the view that the government needs to clarify a number of areas. These are set out below.

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

The Bill clarifies existing provisions in the GDPR that the research provisions for processing data covers privately funded projects in the public interest. It also includes an illustrative and non-exhaustive list of types of scientific research, including technological development, fundamental or applied research or for scientific advances to support public health.

These are pre-existing provisions in the GDPR which have historically been underused; the changes intend to give private sector organisations, which often apply a more risk-averse interpretation of the law, more confidence to use the privileges of the research provisions in the GDPR.

In every single case, the researchers will still have to self-assess whether their project constitutes "scientific research" and adhere to all safeguards in the legislation.

techUK supports these changes and believes that the combination of enhanced legal clarity and incentives for data-driven research, along with the recent expansion of the UK's R&D tax credit to cover data and cloud computing costs, will give the UK a competitive advantage and make Britain an even more attractive destination for conducting crucial research into key areas such as AI, biotechnologies, and medical research.

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. Ensuring the recognised list of legitimate interests works as intended

The Bill will introduce a list of "recognised" legitimate interests for processing data. These include public interests such as national security, public security such as responding to emergencies, helping respond to and prevent crime including economic crimes such as fraud and processing data to support the safeguarding of children or vulnerable adults.

Previously the processing of data for these purposes may have required a lengthy balancing test. By recognising these limited public interest use cases organisations can be more confident when processing data and will not need to carry out lengthy legal assessments, streamlining the process and reducing compliance burdens when being asked to respond to sometimes serious and rapidly moving situations.

As well as the "recognised" legitimate interests list, the legislation outlines examples of processing "that is necessary for the purposes of a legitimate interest."

This is a non-exhaustive list of activities that may be considered legitimate interests. These include direct marketing, intra-organisation data sharing (e.g. between departments), and upholding network and system security. For activities falling under this non-exhaustive list, a balancing test will still be required to ensure that their interests do not override the rights and interests of an individual. However, this non-exhaustive list provides organisations with more clarity on what types of activities are applicable to a legitimate interest meaning they can conduct the balancing test with greater certainty.

Overall, techUK supports the approach taken to legitimate interests and in our view clarifies what was implicit in the existing GDPR regime, giving organisations more certainty over their ability to process data in specific scenarios. The Bill also contains a provision to add or remove recognised legitimate interests following guidance from the ICO and Parliamentary scrutiny.

However, the Government needs to find the right balance on the relationship between Automated Decision Making (ADM) and legitimate interests. It is right that for low risk and regular activities ADM should be available to process data for recognised legitimate interests. This can have major societal benefits, such as helping improve fraud prevention and detection as outlined by one of techUK's members RELX here.Within this context, ADM 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 financial system.For significant or high-risk decisions there needs to be more clarity on how ADM applies to the recognised list of legitimate interests. This is so that citizens have the confidence that a rigorous balancing test is being conducted where there is a chance of a decision being made that has a significant or legal effect and that there are clear avenues for redress.

Beyond the existing recognised list of legitimate interests, the Government should also examine plans to clarify rules around processing personal data for bias mitigation purposes and include this on the face of the Bill. Currently the Bill does not take significant steps to improve how data could be processed to prevent bias in algorithmic or AI systems and this could be improved in further amendments.

3. A more flexible approach to International transfers

techUK welcomes the Government's ambition to move to a more proportionate and risk-based approach to adequacy assessments and data transfer mechanisms, which prioritises both flexibility and the protection of personal data.

This approach aligns with the UK's aims of becoming a global hub for data-driven innovation, and provides additional support for international data transfers. These changes are welcome and needed as the global landscape for international data flows becomes more fragmented, allowing the UK to respond effectively in a changing world.

To further support UK's aims, we recommend the government to take the following steps:

Establish a proportionate increase in flexibility for use of derogations: by making explicit that repetitive use of derogations is permitted, a derogation is an exception to the general rules governing the processing of personal data under the GDPR.

They are permitted in specific situations where strict adherence to the GDPR would be impractical or unnecessary. For instance, a derogation under Art 49(b) UK GDPR allows a company to transfer personal data to a third country without obtaining explicit consent from the data subject if the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request.

Derogations under the GDPR are intended for specific, exceptional circumstances to be used as a last resort measures, and not as a substitute for compliance. Organisations must demonstrate a

compelling reason for their use, ensuring they are proportionate, not broader than necessary, and accompanied by appropriate safeguards to protect personal data.

Currently, the repetitive use of derogations is restricted, burdening businesses that need to carry out atypical international transfers within a limited timeframe. Allowing this would offer greater flexibility in situations where other mechanisms are not feasible or appropriate and improve efficiency and result in cost savings. However, to maintain EU adequacy and uphold robust data protection standards, incorporating clear safeguards is paramount. These safeguards should be supported by comprehensive directives from the ICO and well-defined thresholds to ensure responsible use or derogations. To ensure responsible and proportionate usage, clear safeguards will be crucial, and we would welcome the ICO's guidance with well-defined thresholds.

Exempt 'reverse transfers' from the international data transfer regime, ensuring that the exemption only applies to transfers of personal data that have already been protected in the originating country: Exempting 'reverse transfers' from the international data transfer regime holds immense potential to alleviate the administrative burden on businesses while maintaining robust data protection standards.

Currently, when data is received in the UK and subsequently sent back to the originating jurisdiction, it necessitates the organisation handling the data to find a basis for the data to be returned, even if the data is not changed or edited but no additional personal data is added. This requirement introduces an unwarranted layer of complexity and bureaucracy, hindering efficient data flows.

Exempting reverse transfers would eliminate the need for businesses to navigate a separate set of data transfer rules when returning data to its original source. However, we are of the view that such an exemption should only apply to transfers of personal data that are covered by a lawful basis for the original transfer to ensure that robust data protection standards are maintained.

4. Allowing the UK's Digital ID market to grow

The digital identity measures in the Bill will enable the Secretary of State to exercise governance functions in relation to the digital verification services (DVS) register. In practice, these functions will be undertaken by the Office for Digital Identities and Attributes (OfDIA), initially integrated within the Department for Science, Innovation, and Technology.

This is a crucial step towards a thriving, safe and trustworthy digital identity ecosystem. Such a system will enable real and inclusive economic growth by fostering increased financial inclusion, and the provision of public services by unlocking access to banking, government benefits, education, and many other critical services. Crucially, this will also reduce fraud, and promote digitisation. Examples of use cases include more secure digital payments, KYC for financial services, digital tax filing, streamlined e-government services, and easier disbursement of government benefits.

Once in place, members would welcome further clarity on the powers, duties, functions, and the subsequent funding model of OfDIA. It's important that those investing in the market have clarity and certainty on how digital identity will be effectively governed.

Additionally, we are concerned about potential added bureaucracy when companies must comply with both the proposed Digital Identity Trust Framework for government-approved digital IDs and other sector-specific requirements.

This dual compliance could lead to duplication and excessive administrative burden, especially when other sectors have more extensive demands than the Government ID. We therefore support the Government's amendments to introduce a 'supplementary code' allowing compliant digital IDs from the trust framework to be used across diverse situations, simplifying regulatory compliance.

Protecting citizens and consumers' data rights

Citizens must trust in the UK's data protection regime to maintain consumer confidence in the use of digital products and services and uphold the UK's reputation as a high standard location for storing and processing personal data. This in turn ensures UK companies remain competitive internationally and can continue to innovate.

techUK is of the view that the core principles which underpin the UK GDPR will remain untouched, meaning there is no material lowering of data protection standards in the UK. There are areas of the Bill where tweaks will be introduced to address limitations in the current law, and ensure the legislation is interpreted and implemented as intended.

5. Maintaining EU adequacy

techUK and its members believe that the Bill strikes a good balance between reform and upholding high data protection standards. It is designed to make the UK's data protection regime clearer and easier to comply with, especially for low-risk situations.

The UK government has also stated that maintaining adequacy is a top priority and has been engaging with the EU stakeholders to ensure that the European Commission upholds it.

However, techUK is aware that certain provisions in the Bill, such as those related to automated decision-making, international transfers, and the Secretary of State's powers to approve regulatory codes of practice, have previously raised concerns to the European Commission.

We welcome amendments laid by the Government that will restrict the Secretary of State's role to providing feedback and recommendations on draft codes, rather than having the power to approve them. These amendments represent a significant step towards ensuring a more independent and transparent regulatory process, fostering greater confidence among industry stakeholders. We strongly urge all MPs and peers to support these amendments to safeguard the integrity and effectiveness of the regulatory framework.

The government should continue addressing the remaining concerns and maintain close collaboration with its European partners to preserve the adequacy decision, which is vital for the tech sector's growth and prosperity.

Further areas for improvement and clarification

7. Automated telephone marketing – technical feasibility of new obligations to report on nuisance communications

Clause 89 of the Bill mandates UK telecommunications providers and networks to notify the ICO within 28 days if they suspect someone is violating direct marketing regulations when using their service. The Bill also sets out that failure to report can result in £1,000 fixed penalty, and the steps the Commissioner must take before issuing it.

While techUK welcomes the ambition of this provision, we note that the sector is already well-incentivised and is committing significant resources and working closely with Ofcom to tackle the challenge of unwanted calls. As well as fulfilling existing obligations from Ofcom, there is an existing voluntary technical memorandum of understanding between a number of UK telecoms providers. We therefore question the extent to which new reporting obligations to a separate regulator will help tackle their root cause or reduce their frequency in the longer term.

Additionally, we have significant concerns about the technical feasibility of such requirements, potentially high costs of compliance, the unclear definition of a nuisance call, and the burdensome reporting process. The proposed regulations raise significant concerns for small and medium-sized businesses, which may struggle to shoulder the compliance costs and potential fines associated with these measures. The monitoring and reporting requirements for email marketing are particularly burdensome, as many businesses' current technical infrastructure cannot meet the monitoring standards outlined in Clause 89.

The lack of clear guidelines for determining what constitutes "reasonable grounds" for suspecting a violation of direct marketing regulations is causing confusion and uncertainty for businesses. Without clear examples of what constitutes unsolicited direct marketing, the expectations placed on service providers to identify and report instances of unlawful direct marketing can lead to inconsistent enforcement practices by the Information Commissioner. This inconsistent enforcement could potentially contradict the government's original intentions when drafting the Bill.

The government should reconsider these requirements and develop more effective solutions to the problem of nuisance calls.

We therefore urge the government to engage with the telecommunications providers to find a practical and workable solution. additional measures to prevent actors sending large amounts of call traffic which could be considered suspicious.

8. 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.

The Schedule 12 of the DPDI 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, DSIT, and the 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 healthtech industry in the UK.

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