# Common misconceptions about the Data Protection and Digital Information (No. 2) Bill

Briefing for MPs and Lords

*techUK addresses some of the common misconceptions that have circulated about the Data Protection and Digital Information (DPDI) (No. 2) Bill.*

*Below we outline these with some examples of how our members expect the DPDI Bill to affect the way they manage personal data in the UK.*

## Misconception 1: The DPDI Bill will weaken data protection and safety standards

Maintaining public trust in the UK's data protection regime is essential for preserving consumer confidence in the use of digital products and services. This trust not only upholds the UK's reputation as a high-standard location for storing and processing personal data, but also ensures that UK companies remain competitive internationally, fostering an environment conductive to ongoing innovation.

The UK General Data Protection Regulation (GDPR) gives individuals specific rights over their personal data. These rights include the right to access personal data held about them, the right to be informed about how and why their data is used, the right to have their data rectified, erased, or restricted, the right to object to data processing, the right to data portability, and the right not to be subject to automated decision-making based solely on personal data.

The DPDI Bill maintains these rights. For example, the Bill will:

- Maintain individuals' right to request a copy of their personal data;
- Empower individuals with enhanced data portability rights through Smart Data schemes that enable seamless transfer of personal data across different platforms and services;
- Protect individuals' rights by ensuring they have the right to request human review or challenge any decision made through automated decision-making processes that significantly affects them and with which they disagree.

The Bill will also make important changes to the accountability framework, i.e. how organisations are held to account for how they process data.

The current framework requires organisations to comply with a set of detailed requirements, generally regardless of the risk associated with their data processing activities. This places a disproportionate burden on SMEs and organisations that undertake low-risk processing.

The proposed changes aim to introduce a more risk-based and adaptable approach to data protection and management, enabling organisations to tailor their compliance efforts to their specific circumstances and foster a robust and risk-driven approach embedded within their operations.

This approach will place a stronger emphasis on the fundamental principles of accountability, including leadership and oversight, risk assessment, policies and procedures, transparency, staff training and awareness, and monitoring, evaluation, and improvement.

For example, even though businesses will no longer be mandated to have dedicated data protection officers, they will be required to designate a Senior Responsible Individual who will be responsible for embedding a data protection-conscious culture within the organisation.

Given that all employees must be actively engaged in data protection to some extent for it to be effective, we view this as a positive step. Similarly, even though businesses will no longer be required to carry out Data Protection Impact Assessments (DPIAs), they will still be required to identify, manage, and mitigate data risks. The steps organisations need to take to comply with these new requirements will be set out in guidance by the ICO, updating existing guidance already in use.

We expect that the overall effect of these changes will mean a more risk-based approach to data governance with organisations who do not process large quantities or sensitive personal data likely seeing a reduced level of compliance burden suitable to their needs.

For organisations that process large amounts of data or those that process sensitive data the changes proposed by the Bill are not expected to present a significant departure from the current framework and may result in some more specific guidance from the ICO.

Having discussed the proposed changes to the accountability framework extensively with our members the vast majority do not expect these changes to affect their approach to data governance as they expect to be held to the strongest standards and will have to build a globally facing compliance approach that meets the needs of multiple jurisdictions.

This is consistent techUK's members views on the Bill as seeking to maintain important data flow agreements, such as EU data adequacy, while seeking to minimise burdens on businesses who do not engage in risky data processing.

## Misconception 2: the Bill will negatively impact EU data adequacy decision

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, with a particular focus on 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.

Adequacy is a flexible designation granted to the UK and 14 other non-EU countries, each operating under its distinct legislative framework. Therefore, we expect that despite the proposed amendments to the Bill, the UK's data protection standards will remain more closely aligned to the EU's than any other nation currently holding an adequacy decision. The high threshold for the potential revocation of adequacy not only ensures that the likelihood of losing this status is minimal but also provides valuable flexibility for implementing necessary reforms.

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.

TechUK urges the government to continue addressing these 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.

## Misconception 3: the Bill will be burdensome on businesses and require dual compliance with both EU and UK regimes

The Bill streamlines and reduces the complexity of the EU GDPR in less risky scenarios, while upholding stringent data protection standards for those who process large quantities or more sensitive categories of data. It also incorporates numerous clarifications and incorporates various GDPR recitals directly into the operational text.

Many organisations operating internationally will maintain an EU standard data protection compliance framework. Changes in the DPDI Bill (No.2) have been drafted with this in mind and will enable organisations complying with EU law to by default comply with the new UK GDPR.

There are some exceptions such as the requirement to designate a Senior Responsible Individual, however techUK expects guidance from the ICO to allow for small differences to be resolved relatively easily.

We expect this would be done in a similar way to recent actions taken by the ICO to bridge gaps between the UK's and EU's regimes that have already materialised on international data transfers.

The construction of the DPDI Bill and pragmatic steps by the regulator should reduce the need for businesses to contend with dual compliance requirements.

## Misconception 4: the DPDI Bill provide little benefit to businesses - research provisions

The UK's leadership in research and development has been pivotal in maintaining its global competitiveness and appeal to international talent and investment. Data and AI driven R&D is an integral aspect of this, and the DPDI reforms directly support this by clarifying that the definition of scientific research includes research carried out as a commercial activity, but clarifying that research into public health will only count as scientific research if it is in the public interest.

The Bill also includes an illustrative and non-exhaustive list of examples of scientific research, such as applied or fundamental research, or innovative research into technological development. We welcome

this clarification and expect it to instill confidence in researchers, promote a more risk-tolerant interpretation of the law, and encourage heightened participation in research initiatives.

Furthermore, the benefits of these provisions are not solely commercial, but also have huge opportunity for societal gain, fraud prevention, increasing competition, protecting the vulnerable and wider public interest, and crisis management. We set some use cases below that would have benefited from the greater clarity proposed by the Bill:

- **Enhancing the understanding of consumer behaviour:** Google Places API and Google Trends have been used by institutions such as the International Monetary Fund to better understand consumer spending patterns during the pandemic, and how businesses were coping during lockdowns.
- **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 is an award-winning crowdsourcing app, developed by Vodafone Foundation, that uses the processing power of mobile phones to accelerate scientific research. For cancer research, DreamLab has identified over 110 anti-cancer molecules and potential reproposed drugs, while for COVID-19 research, the app has employed AI to analyse virus-host interactions data, identifying potential antiviral treatments.

The changes proposed by the DPDI Bill alongside the recent expansion of the widely used R&D Tax Credit to cover data, cloud computing and mathematics expenditures will make the UK an attractive place for data and AI driven R&D delivering the UK a significant competitive advantage in a key growing part of the global economy.

## Misconception 5: the changes to legitimate interests is a significant departure from the GDPR and creates a free for all in data processing

Legitimate interests is one of the original grounds for lawful processing of personal data contained within the GDPR.

Legitimate interest processing is used to process personal data in ways that the data subject would reasonably expect and which have a minimal privacy impact, or where there is a compelling justification for the processing. Using legitimate interests often requires an organisation to use a balancing test, i.e. providing reasoning for the processing.

However, an overly cautious approach to data governance has often meant that this lawful basis is underused and causes caution among organisations, slowing down services and innovation that the law intended to take place.

The DPDI No.2 Bill seeks to clarify and improve the use of legitimate interests in two ways.

The first is by through a list of "recognised" legitimate interests. This recognised list sets out a range of non-commercial interests including national security; public security (such as responding to emergencies and preventing crime, including economic crimes such as fraud); and processing data to support the safeguarding of children or vulnerable adults.

The law clarifies that these purposes do not require a balancing test and therefore provides organisations with greater certainty that data can be processed in these public interest, and often time sensitive scenarios.

The second change the DPDI Bill makes is to provide illustrative examples of legitimate interests such as direct marketing, network security and intra-group transfers. Using legitimate interests for these purposes still requires a balancing test, however by providing greater clarity on the intention of the law organisations have greater confidence that a balancing test is appropriate for a range of scenarios.

techUK members have highlighted the following scenarios where these changes to legitimate interest will improve the UK's data protection regime:

- Enhancing fraud prevention and detection and providing organisations with legal clarity and simplifying compliance while bolstering their capacity to deter online fraud. For instance, LexisNexis Risk Solutions' Digital Identity Network, a RELX subsidiary, has been successful in detecting and preventing fraudulent transactions through data sharing.
- Improving the safety and security of their products and services by using data to identify potential security risks;
- Improving user experience by enabling companies to personalise services and provide more relevant recommendations.

Furthermore, the proposed changes are necessary for operationalising some of the ambitious legislation that the government has legislated for, including the Online Safety Act and for supporting the government's strategy on fraud.

New legitimate interests can be added to exhaustive list, however doing so would require these to be laid before Parliament and for advice to be provided by the ICO on the appropriateness of the proposed change.

We therefore see the DPDI's approach to clarifying legitimate interests as in line with the approach envisaged by the GDPR and with safeguards and accountability for future changes.

## Misconception 6: automated decision making will negatively impact the rights of data subjects

Under the DPDI updates, data subjects will continue to be able to contest an automated decision making (ADM) and instances of profiling, but only when it could lead to a decision with significant or legal effect. This will establish a difference between low-risk ADM's which are now integrated in our everyday lives, such as service personalisation, from high-risk ADMs that seriously impact an individual's life, such as mortgage reviews or technologies that aid with hiring and employment.

Automated decision-making (ADM) is becoming increasingly integrated into consumers' daily digital interactions, providing organisations with valuable tools to enhance user experiences.

The majority of ADM are for low-risk basic functions, from tailoring personalised content to supporting faster logins to performing light and non-consequential checks, for example estimating whether someone would be successful in a credit application. ADM when combined with other parts of the Bill, such as the legitimate interest provisions can also be an effective tool in helping scan, prevent and mitigate fraud.

Though we welcome the transformative potential of ADM, 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.

Therefore, some further changes are needed in the Bill, such as clarifying how ADM applies to the recognised list of legitimate interests. 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.

Additionally, we will want to see the fast introduction of avenues for redress of AI based decisiosn as proposed in the Government's whitepaper, as this will be important to complement the DPDI Bill.

### Misconception 7: changes to the international transfers regime are not appropriate or accountable

In today's interconnected world, the seamless flow of data across borders is crucial for innovation and economic growth. This is especially important in the increasingly uncertain world, where recent trends have raised concerns about the proliferation of data localisation requirements and increased barriers to cross-border data flows.

This is illustrated by recent OECD findings, which show that 19 OECD nations identified ambiguity surrounding legal privacy frameworks as a primary obstacle to cross-border data movements, with "Incompatibility of legal regimes" being cited by 16 countries as another significant challenge.1

To tackle these challenges head on, the UK needs to have a flexible and adaptable approach.

The DPDI Bill will provide the UK with that flexibility as it marks a shift to a more risk-based approach to data adequacy decisions, such as by developing a more flexible and outcomes-based approach for assessing jurisdictions for adequacy. Additionally, the law will allow for the UK Government to adopt more varied forms of safeguards for global transfers. This will allow us to keep pace with an ever-changing world.

The Government's Independent International Data transfers Expert Council set out that a flexible and accountable approach to data transfers was vital for the more fragmented world we expect to see develop in their recent report.

Overall, we believe the DPDI Bill finds a good balance. However, the Bill does grant increased power to the Government, and the Parliamentarians must therefore be ready to scrutinise any future changes enacted utilising the accountability mechanisms contained in the Bill. These include guidance from the ICO and

[1] OECD: Digital Economy Outlook 2020, fig 6.4

parliamentary oversight. This will help ensure the evolution of the UK's international data transfer framework works for citizens and businesses.