

The Data Protection and Digital Information Bill

One final push needed to reap the full benefits of reform

September 2022

Following withdrawal from the European Union (EU), the UK has the opportunity to develop a custom data protection regime that works better for British businesses, while maintaining a globally recognised high standard of data protection rights and preserving data flows with our international partners including the EU.

Since its adoption in 2018, the UK's General Data Protection Regulation (GDPR) has had limitations, with organisations of all sizes citing a lack of certainty and clarity as holding them back from innovating with data, and smaller firms unable to absorb the more onerous compliance requirements of the regime. Its design and implementation has also had unintended consequences within certain supply chains, particularly where there are pre-existing competition concerns.

With the EU set to review its own GDPR in 2024 and discussions starting sooner, the UK is in a unique position to be a global leader on future data governance and set a new standard for data protection that is better suited for our modern digital economy. We therefore welcome the Secretary of State's aim to use the Data Protection and Digital Information Bill (DPDI) to update our laws and create a new British data protection system.

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. These include ensuring individuals can access their data and have reliable avenues to seek redress, for example by ensuring human review of automated decisions where there is a legal or similarly significant effect.

In the DPDI Bill, techUK members believe the Government has struck a sensible balance between the changes we need to better enable data-driven innovation such as artificial intelligence, cutting-edge R&D and Smart Data schemes while preserving data protection rights.

However, as the new Government has paused to reflect on the DPDI Bill, there is an opportunity to review its contents to ensure the full benefits of reform are reaped without threatening data protection rights, or the EU's positive adequacy decision. Doing so will help the UK unlock the full value of data across the economy, provide regulatory comfort that supports bold investment decisions, and help deliver on the ambitions of the National Data Strategy as well as the Government's desire for growth in the digital economy.

These include:

- 1. Broadening and clarifying the research provisions to offer organisations certainty when conducting data-driven, commercial R&D;**
- 2. Expanding the legitimate interest list to allow organisations to more easily secure their networks and improve their internal systems;**
- 3. Providing additional flexibility for international data transfers to allow the UK to become a global hub for data-driven innovation;**

4. **Ensuring Regulatory coherence between data protection legislation and the UK's AI Governance policy;**
5. **Delivering a clear, innovation-enabling framework for digital verification services which helps to lower barriers to entry for new market entrants and promotes growth and competition;**
6. **Clarifying the Secretary of State's new regulation making powers, particularly the intention for the Secretary of State to approve the regulator's statutory codes of practice;**
7. **Commitment to further consultation on the long-term move to an opt-out model for cookie consent;**
8. **Removing additional barriers to security updates on-device, to ensure end-users remain protected against security vulnerabilities;**
9. **Narrowing the scope and clarifying obligations for communications providers to report on unsolicited directing marketing;**
10. **Clarifying how new information standards for health and social care will interact with the draft Standards and Interoperability Strategy.**

With the DPDI Bill intending to implement changes which seek to reduce burdens of the existing legislation (DPA 2018), most organisations will be able to take advantage of new benefits as soon as the Bill is adopted. To ensure these benefits are maximised, the Government should seek to resume the Bill's Parliamentary passage as soon as possible, to provide the regulator sufficient time for its own restructuring, and to develop the necessary guidance to help businesses implement the new regime.

1. Broadening and clarifying the research provisions to offer organisations certainty when conducting data-driven, commercial R&D;

The ability to conduct data-driven R&D is seen as one of the prizes of reform and will be key in supporting the UK achieve its ambition to be a science superpower. While techUK has welcomed the Government's proposal to use Recital 159 as the basis for introducing a definition of "scientific research" into the legislation, there is still a lack of clarity on the scope of this definition, and the extent which it will include commercially funded research and data science.

Although the Government has expressed its intention for the definition to be understood in the "broadest sense", there is a possibility that organisations will continue to take risk-averse approaches to R&D, a challenge which this provision is seeking to tackle. To ensure the reform is understood and implemented as intended, the Government could consider making explicit reference to "product development and data science" in the definition of scientific research.

Regulatory guidance, with clear examples will also be key for organisations to implement the new regime with certainty.

2. Expanding the legitimate interest list to allow organisations to more easily secure their networks and improve their internal systems;

The introduction of a limited, exhaustive list of legitimate interests, no longer requiring a balancing test is a proposal techUK members have long called-for. While techUK

envisaged for this to be a much more ambitious list of processing activities, we welcome the Government's intention to include processing activities which supports the public interest as well as the flexibility within the law which will allow new items to be added with time, and with appropriate safeguards in place.

As the Government reviews this proposal, it should consider including new public interest items to the list such as:

- **Network security**, which will enable organisations to maintain the cybersecurity of their systems and that of their customers. All organisations should deploy cybersecurity capabilities to protect data, systems, and infrastructure, and this requires the sharing of cyber threat information and the monitoring networks, systems and devices for unusual behaviour and preventing unauthorised access. To perform such functions, organisations must process data, including data from customers, employees or third parties. For example, this includes scanning IP and metadata on endpoints to check for malicious activity or scanning applications in the cloud to ensure they have not been compromised. All of which is necessary to protect organisations from cyberattacks. Recital 49 of the EU GDPR references the need for organisations to be able to process "personal data to the extent strictly necessary and proportionate for the purposes of ensuring network and information security, and we urge the UK Government to replicate this approach in the revised Bill.
- **Internal research**, which will enable organisations to carry out workplace equality assessments and research into inclusion and diversity of their workforce. This will help improve people and workplace management; a vital aspect of how companies seek to improve their productivity.

Finally, for this list to be effective, organisations must be able to use automated decision-making to carry out these processing activities. For example, many organisations will depend on AI systems to detect fraud in their systems and would only benefit from the legitimate interest list if automated decision making was in scope. Currently, it is not clear whether this is the case and Government should set out that automated decision making is within scope. This will not undermine privacy as citizens will still have the ability to ask how their data is being used and seek redress under the proposed new regime.

3. Providing additional flexibility for international data transfers to allow the UK to become a global hub for data-driven innovation;

While techUK has welcomed the Government's ambition to move to a more proportionate and risk-based approach to adequacy assessments and data transfer mechanisms, it was disappointing to see widely supported proposals dropped from the *Data: a new direction* consultation. The Government should consider reintroducing these proposals into the DPDI Bill:

- **Repetitive use of derogations**, which will help to reduce burdens on businesses caught short by a need to carry out atypical international transfers for a limited period of time. The ICO will be able to set out guidance with clear thresholds around the use of these derogations, so they are used only in appropriate circumstances. As it stands, the EU GDPR is too restrictive in their use and the UK could support organisations by allowing more flexibility, but with clear safeguards.
- **Exempting reverse transfers from the international data transfer regime**, (i.e., data originating outside of the UK, sent to the UK, and back to the originating

jurisdiction) which would significantly reduce burdens on businesses without undermining data protection standards.

If introduced, both provisions would require further regulatory guidance.

4. **Ensuring regulatory coherence between data protection legislation and the UK's AI Governance policy;**

As the Government develops its approach for future AI Governance, regulatory coherence between data protection and AI regulation will be crucial for ensuring innovation is not stifled.

The Government must consider how a decentralised approach to AI regulation will interact with the GDPR i.e., Article 22 and how to mitigate the risk of creating further uncertainty or conflicting compliance requirements for organisations seeking to innovate with personal data and AI.

The Government should also bring forward plans to clarify rules around processing sensitive personal data for bias mitigation purposes and include this on the face of the Bill. techUK and our members would be happy to suggest amendments or engage with officials how these changes should be designed.

5. **Delivering a clear, innovation-enabling framework for digital verification services** which helps to lower barriers to entry for new market entrants and promotes growth and competition;

techUK welcomes the Government's intention to develop legislation to support the UK Digital Identity & Attribute Trust Framework, (the 'Framework' hereinafter). However, members have highlighted several areas of concern which could impact the effectiveness of the Framework and the UK Digital ID ecosystem if not addressed within the Bill. The Government should consider:

- **Developing a Registry Levy that is fair and proportionate** to keep market barriers to a minimum and to ensure small players can continue to have market access, which is critical for stimulating competition and innovation.
- **Ensuring coherence** between the UK GDPR and the Framework to avoid the risk of gold plating existing data protection rules, creating duplicative or conflicting compliance requirements as well as uncertainty for digital ID providers and end users.
- **Clarifying the scope of the trust mark** by ensuring it extends to both relying parties and end-users, potentially as a registered trademark. The Government must also help to build public support for Digital Identity, by publicly promoting the benefits of the trust mark.
- **Creating a robust DVS register, with appropriate safeguards in place** by mandating national security and sanctions checks for applicants of the DVS register and developing a clear appeals process should the Secretary of State withdraw a Framework participants' certification, regardless of reason.
- **Recognising Digital ID as critical national infrastructure** to acknowledge its importance in allowing UK citizens to verify their identities in an online environment, and contribution to a thriving digital economy.

Overall, there is a deep concern that the lack of industry consultation for this section of the Bill could lead to a Digital ID ecosystem that is stunted in terms of growth, innovation, and competition. techUK welcomes the opportunity for dialogue with DCMS teams working across Digital ID and the DPDI Bill.

6. Clarifying the Secretary of State's new regulation making powers, particularly the intention for the Secretary of State to approve the regulator's statutory codes of practice;

While techUK welcomes the flexibility that will be introduced to the data protection regime through new Secretary of State powers, these must remain underpinned by clear safeguards such as consultation with the regulator, affirmative parliamentary procedures, and prior industry consultation.

This will be particularly important when introducing new sector-specific Smart Data schemes, which will require close collaboration between Government and industry to ensure smart solutions are proportionate to implement and provide real benefits to consumers.

There is also a real concern that the ability for the Secretary of State to approve the regulator's statutory codes of practice could result in scenarios where Government is casting judgement on its own data protection responsibilities, and consequently threaten the independence of the regulator, which is key to maintaining the EU's positive adequacy decision. The Government should provide further clarity on when and how this power would be exercised, including what safeguards will be in place to avoid misuse.

7. Commitment to further consultation on a long-term move to an opt-out model for cookie consent

techUK welcomes the Government's desire to explore ways to reduce "consent fatigue" caused by cookie banners required under PECR legislation. However, there are concerns about the Government's decision to move towards browser-enabled models for managing user consent, despite industry consultation responses raising concerns and the lack of further consultation before publication of the Bill.

Before the Government develops its thinking on this topic further, it is essential for there to be open and broad consultation with industry to fully understand their concerns. The Bill does not propose change to PECR rules themselves and services providers' legal responsibilities remain. Providers also have legitimate concerns about browsers intermediating their relationship with customers. Separately, the CMA has investigated competition concerns in the browser market, so Government must avoid further market distortion via regulation. Other potential challenges include interoperability with international laws, technological readiness of browser-based solutions, as well as impact this could have on innovation.

8. Removing additional barriers to security updates on-device, to ensure end-users remain protected against security vulnerabilities

techUK welcomes an expansion of the exemption to the cookie consent requirements under PECR legislation. However, there are concerns that the proposed exemption for security updates in s.79 of the Bill (the new Regulation 6(2C)) would, in fact, serve to narrow the existing rules and jeopardize consumer security.

It has been widely accepted (supported by ICO guidance) that storing information on a user's terminal equipment for security purposes meets the existing "strictly necessary" exemption in PECR. Consequently, these updates should not require user consent under the existing law. Whilst techUK welcomes explicit confirmation of this in the Bill, the standalone exemption for this purpose introduces additional conditions which are not present in the existing law, including the requirement to offer users an opt-out from the security update and the ability to disable or postpone it. Although techUK recognizes the value of user choice, where a software update satisfies the condition of being necessary to ensure the security of the terminal equipment, offering an opt-out risks leaving users vulnerable to known security flaws. There is also concern that this exemption substantially overlaps with the new examples of strictly necessary purposes in paragraph 5, creating confusion.

The Government should consider removing the opt-out requirements from this new exemption, or else simply explicitly clarifying that this purpose is already exempt due to being strictly necessary.

9. Narrowing the scope and clarifying new obligations for communications providers to report on unsolicited directing marketing.

In Part 4, Clause 85 of the DPDI Bill, new obligations have been introduced for communications providers to report on "suspicious activity" related to unsolicited direct marketing to the ICO which could include calls, SMS, and emails. Suspicious activity must be reported to the ICO within 28 days of the provider first becoming aware of it, and the ICO may impose fixed penalties for non-compliance.

While techUK welcomes the ambition of this provision, the sector is already committing significant resources, is well incentivized and working closely with Ofcom to tackle the challenge of unwanted calls and questions 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. As well as fulfilling obligations to identify and prevent suspicious calls to Ofcom, there is an existing voluntary technical memorandum of understanding between a number of UK telecom providers who take additional measures to prevent actors sending large amounts of call traffic which could be considered suspicious.

As the Bill is reviewed, there are several aspects of this provision which need addressing within the legislation and where further consultation with industry would be welcomed prior to receiving regulatory support and guidance:

- **Narrowing the scope and clarifying definitions in the Bill:**
 - to make clear that communications providers will not be obligated to monitor the content of individual electronic communications to determine whether they contravene PECR legislation.
 - to include on the face of the Bill, a clear definition of what is meant by "suspicious activity" as well as a specific legal threshold for communications providers to have a "reasonable suspicion" that such activity is occurring.
 - to remove e-mail from the scope of the requirements in Clause 85. It is not technically possible to use the same approach to determining "reasonable suspicion" as can be applied in the case of Voice and SMS.
- **More transparency on policy design;** it is unclear if an impact assessment was carried out for this proposal, whether industry and/or law enforcement agencies

were consulted prior to the Bill's publication, and what other policy options were considered, if any at all.

- **Further consultation with industry** to ensure any new obligations are proportionate, not duplicative, technically workable and do not create any privacy or security concerns.

10. Clarifying how new information standards for health and social care will interact with the draft Standards and Interoperability Strategy

techUK understands and supports the intention behind the proposed legislation for health and social care. In fact, [techUK's Interoperability Charter for Health and Social Care](#) was developed to help achieve the aims set out in the DPD Bill. However, as many have been highlighting over the years, interoperability is much more than just a technical problem. Enforcing a set of standards that suppliers have to meet and imposing financial penalties will not help on its own to drive adoption. We strongly encourage NHS England and DCMS to work closely with suppliers and help to build trust and ultimately drive progress in the space. techUK is preparing a separate paper on the challenges suppliers are highlighting to us solely on the health and care sections of the Bill. This includes:

- **Addressing challenges arising from the proliferation of frameworks** and lack of alignment on interoperability, meaning suppliers working under different contracts will be required to deliver different things
- **Ensuring there is consistency in clinical workflows** in the areas where standards are to be enforced, and to specify data flows required, committing to generating that data
- **Defining standard APIs** through which FHIR UK Core resources will be accessed
- **Providing a clear understanding of the introduction of the information standards**, with associated timelines.

techUK welcomes further engagement with the supplier community 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.