techUK

techUK.org | @techUK

Data Protection and Digital Information No. 2 Bill

techUK's written submission to the Public Bill Committee, DPDI No. Bill

May 2023

Contact: Dani Dhiman, Policy Manager - Data
T 020 7331 2000 | E dani.dhiman@techuk.org

techUK

techUK.org | @techUK

About techUK

techUK is a membership organisation launched in 2013 to champion the technology sector and prepare and empower the UK for what comes next, delivering a better future for people, society, the economy, and the planet.

It is the UK's leading technology membership organisation, with more than 900 members spread across the UK. We are a network that enables our members to learn from each other and grow in a way which contributes to the country both socially and economically.

By working collaboratively with government and others, we provide expert guidance and insight for our members and stakeholders about how to prepare for the future, anticipate change and realise the positive potential of technology in a fast-moving world.

Contact: Dani Dhiman, Policy Manager - Data
T 020 7331 2000 | E dani.dhiman@techuk.org

techUK

techUK.org | @techUK

The benefits of the UK's new data protection laws are ready to be seized

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

There are limitations to the UK's General Data Protection Regulation (GDPR), adopted in 2018, 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. With the EU set to review its own GDPR in 2024-5, 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.

The Government's Data: a new direction consultation tested proposed reforms through over 40 stakeholder roundtables facilitated through the National Data Strategy Forum, and almost 3,000 responses to the written consultation itself. The proposals pulled on best practice from jurisdictions around the world such as Singapore and New Zealand, as well as emerging EU case law (i.e., changes to Article 22 follow approaches seen in the Netherlands).

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 policy challenges including economic stability, the fight against cancer, financial exclusion, and combating fraud. 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 risk-based approach for SMEs and small organisations e.g., a hairdressers or MP's office.

Clarifying the research provisions of the UK GDPR; All organisations will receive more clarity and legal certainty on how and when they can conduct scientific research, i.e. medical trials, train responsible AI algorithms, or product development. This will 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. These changes will provide an essential competitive advantage to companies operating in the UK, which funded over £25 billion of UK R&D in 2018[1].

Examples of commercial R&D powered by data

- **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.

[1] UK Research and Development Roadmap - GOV.UK (www.gov.uk)

Contact: Dani Dhiman, Policy Manager - Data
T 020 7331 2000 | E dani.dhiman@techuk.org

- **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. It launched in the UK in 2018 to facilitate cancer research.

- **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.

- **Onfido's product development**, UK-based digital identity verification service provider conducts research into AI bias mitigation and algorithmic performance optimisation to continually improve its offering.

- **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.

Introducing a legitimate interest list: Inspired by the Singaporean model, this provision will tackle the over-use of consent, allowing organisations to conduct common-purpose processing activities that have a clear public interest without the need for lengthy legal assessments i.e., detecting economic crime, safeguarding children, public safety.

The Bill will also give clear examples of common-purpose business services that may be considered a legitimate interest including direct marketing, intra-organisation data sharing (i.e., from one department to another), and upholding the security of networks and systems. Here, a balancing test is still required, but will provide organisations with more clarity on what types of activities are applicable to a legitimate interest.

Examples of the legitimate interest list in practice

One of the proposed processing activities under the legitimate interest list, no longer requiring a balancing test is detecting economic crime. This could be significant in providing organisations tackling online fraud with more legal certainty when using personal data, while reducing the compliance burdens of lengthy legal assessments:

- **VISA's anti-fraud detection system** has helped reduce its global fraud rate by two thirds and prevented an estimated $25 billion in fraud in 2019.

- **LexisNexis Risk Solutions' Digital Identity Network, part of RELX** is helping to identify and prevent fraudulent transactions through data sharing, without impairing customer experience of privacy.

Contact: Dani Dhiman, Policy Manager - Data
T 020 7331 2000 | E dani.dhiman@techuk.org

Cutting the red tape for compliance: Organisations will be able to tailor their data protection compliance framework with the level of risk associated with their processing. This means a low-risk business (such as an SME), will not require the same level of compliance as a global corporation.

In the DPDI Bill II, the Government has sought to further lessen burdens for small, low data-intensive businesses by only requiring responsibilities such as risk assessments, record-keeping, and the need for a senior responsible individual when high-risk data processing is taking place. Regulatory guidance will be key in outlining to businesses what constitutes "high risk processing."

Protecting citizens and consumers' data rights

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. Some commonly raised examples:

- **Subject Access Requests:** Data subjects will continue to be able to ask controllers how their data is being collected and stored. At the same time, organisations will be empowered to refuse or charge a reasonable fee for an excessive or vexatious request – these refer to requests not made in good faith i.e., to intentionally cause distress, to be used as a pre-litigation mechanism, or are repetitive in nature. One techUK member received and responded to around 160,000 subject access requests from UK customers in 2022 at the end of Q3 2023.

- **Article 22 (the right to a human review of automated decision making (ADM)):** data subjects will continue to be able to contest an automated decision and instances of profiling, but as stated in the Bill, now 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 with high-risk ADMs that seriously impact an individual's life, such as mortgage reviews or technologies that aid with hiring and employment.

- **Secretary of State powers:** In many parts of the Bill, regulation making powers are welcomed as they will ensure the legislation can remain agile, future-proof, and able to keep at pace with innovation. In every case, the Secretary of State will be legally required to consult with the regulator and relevant bodies before issuing a change, and MPs will be able to have a say through an affirmative parliamentary procedure.

- **Research provisions:** the Government will not be broadening the definition of scientific research but clarifying that it does (and always intended to) capture privately funded

Contact: Dani Dhiman, Policy Manager - Data
T 020 7331 2000 | E dani.dhiman@techuk.org

projects in the public interest. These are pre-existing provisions in the GDPR which have historically been underused; the changes simply intend to bring private researchers more confidence when interpreting the law. In every single case, the researcher will still have to self-assess whether their project constitutes "scientific research" and adhere to all safeguards in the legislation.

Areas for improvement/clarification:

While the direction of the Bill is positive, it remains unclear how some of the reforms that the Bill legislates for will work in practice, including:

- Senior responsible individual (Clause 14)
- Proposals to create an opt-out system for cookies (Clause 79)
- Exemptions for cookie requirements (Clause 79)
- Technical feasibility of new obligations to report on nuisance calls (Clause 85)
- Smart Data (Part 3, Clause 62)
- Security breach reporting, PECR (to consider adding to the Bill)

Senior responsible individual (Clause 14): Currently, UK data protection law does not explicitly require Data Protection Officers (DPO) to be part of senior management. In fact, a DPO who also holds a senior management position may give rise to conflict of interest. Therefore, we are concerned that the Bill's requirement that a senior responsible individual must be part of senior management may create a level of conflict and duplication for organisations that operate across the EU and UK.

While techUK understands the Government's intention not to introduce duplicative compliance requirements for companies operating in the UK and EU, clarification in the Bill text on whether both a senior responsible individual and a DPO (for EU GDPR purposes) are required would be welcomed.

Proposals to create an opt-out system for cookies (Clause 79): techUK welcomes the Bill's intention to address the challenges around consent fatigue and is pleased that the Government has acknowledged the complexities that underpin browser-enabled models, such as competition concerns in the browser market as well as challenges related to liability, technical workability, and interoperability with international standards.

It is critical that the Bill requires the Secretary of State to consult before implementing any new browser-based consent regulations and consider other mechanisms to achieve the aims of the provision. For example, the Government could prioritise expanding the list of exceptions to the consent requirements for cookies and other technologies under PECR instead.

The Bill should add an obligation that requires the Secretary of State to consult with providers, the CMA and ICO before implementing any browser-based consent regulations. This should include browser providers, as well as publishers reliant on online advertising to fund their services.

Contact: Dani Dhiman, Policy Manager - Data
T 020 7331 2000 | E dani.dhiman@techuk.org

Exemptions for cookies (Clause 79): techUK welcomes an expansion of the exemption to the cookie consent requirements under PECR legislation. However, as currently drafted, the legislation unintentionally excludes low-risk and critical activities.

- **Definitions:** Use of the term 'information society service' (ISS) could exclude a small local business operating a website to provide information about opening times or their stock or service availability.
  - Use a more general term such as "service".

- **Software security updates:** Requiring providers to offer users a "simple means of objecting" to an update, risks leaving their devices being exposed to security vulnerabilities. Here:
  - Remove the requirement to allow users to opt-out of software security updates or to not make changes if it affects users' privacy, by removing subparagraph 2C and including a statement in the Bill that software security updates are a "strictly necessary" purpose.
  - Alternatively, security software updates could be added to the list of examples of strictly necessary purposes in the new regulation 6(5).
  -

- **Analytics cookies:** The new exemption to the 'cookie consent' requirement only allows for information to be collected for "statistical purposes", which will exclude a large portion of benign analytics cookies use by websites today and will have limited impact on the Government's goal of reducing "consent fatigue". Here:
  - Replace "statistical purposes" with" analytical purposes".
  - Remove or broaden the condition that analytics data can only be used with a view to make improvements to the service/website/app.
  - Remove the restriction on sharing or else limit sharing to data processors **and/or** only apply to personal data.

Technical feasibility of new obligations to report on nuisance calls (Clause 85): While techUK welcomes the ambition of this provision, the sector is already well incentivised and is committing significant resources and working closely with Ofcom to tackle the challenge of unwanted calls. 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. As well as fulfilling existing obligations from 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.

Contact: Dani Dhiman, Policy Manager - Data
T 020 7331 2000 | E dani.dhiman@techuk.org

As the Bill is reviewed, we encourage the Committee to consider the following amendment to the legislative text:

> (2) After regulation 26 insert— "26A Duty to notify Commissioner of unlawful direct marketing
>
> (1) A provider of a public electronic communications service must notify the Commissioner of any reasonable grounds the provider has for suspecting that a person is contravening or has contravened any of the direct marketing regulations in the course of using the service for calls.
>
> (2) A provider of a public electronic communications network must notify the Commissioner of any reasonable grounds the provider has for suspecting that a person is contravening or has contravened any of the direct marketing regulations in the course of using the network or using a public electronic communication service provided by means of the network for calls.
>
> (3) The network or service provider will not be required to intercept or examine the content of the communication.
>
> (34) A notification under this regulation must be given within the period of 28 business days beginning with the day on which the reasonable grounds for suspicion come to the attention of the provider.
>
> (4 5) "Direct marketing regulations" means regulations 19 to 22.
>
> (6) Subsections (1)-(4 5) above come into force at the end of the period of one year beginning with the day on which the Commissioner produces and publishes the guidance referenced in Regulation 26C

Smart Data (Part 3, Clause 62): techUK has called on Government to introduce economy-wide Smart Data schemes which will drive economic growth, competition, and innovation, while bringing consumers real benefits.

This enables a flexible approach, which means funding models will be determined by the respective Secretary of State when designed, with specific sector dynamics kept in mind. While we welcome this flexibility, this approach has created uncertainty for businesses and investors who could expect a Smart Data scheme to be introduced to their sector at any time.

There are also concerns that without requirements to properly consult industry, conduct rigorous cost-benefit analyses and impact assessments, new Smart Data schemes could incur businesses significant cost and resources to set up data sharing infrastructure, and not bring consumers any real benefits.

To address these concerns and bring industry certainty, the Government should set out a clear plan for the implementation of Smart Data, signaling which sectors it will prioritise and a timeline of when schemes will be introduced, and the Bill should require the following:

- To clause 62 (4) add The Secretary of State or the Treasury shall decide to make regulations under this section only if – (i) an impact assessment has been undertaken by

Contact: Dani Dhiman, Policy Manager - Data
T 020 7331 2000 | E dani.dhiman@techuk.org

or at the direction of the Secretary of State or the Treasury; and (ii) based on the findings of such impact assessment, the Secretary of State or the Treasury is satisfied that the likely benefits outweigh the likely costs.

- A new clause should be added stating (a) The Secretary of State or the Treasury may direct a competent authority to exercise the power to make provision in connection with customer data under this section. (b) Where the Secretary of State or the Treasury directs a competent authority under subsection (5)(a), reference to "regulations" under this Part means 'such conditions as the competent authority may impose in exercising the power under subsection (5)(a)' and reference to "the Secretary of State or the Treasury" means such competent authority.

Security breach reporting, PECR: The DPDI No. 2 Bill presents an opportunity to significantly reduce the administrative burden of PECR security breach reporting on the ICO and communication service providers (CSPs) while still maintaining a high standard of protection under the GDPR's breach reporting rules.

Currently, Reg 5A PECR requires CSPs to: (i) report personal data breaches occurring in connection with their service to the ICO within 24 hours of detection and (ii) notify individuals of a breach where it is '*likely to adversely affect*' their personal data or privacy. Neither of these obligations has a materiality threshold, which contrasts with: (i) Art 33 GDPR, which requires '*a risk to the rights and freedoms of individuals*' before a breach becomes reportable to the ICO and (ii) Art 34 GDPR, which requires a '*high risk to the rights and freedoms of individuals*' before it becomes notifiable to data subjects. This means that CSPs typically report far more data breaches under PECR than the GDPR, and the majority of those reports relate to trivial breaches involving the unauthorised disclosure of limited non-sensitive data that are quickly remedied (e.g., a single email containing a first name and address being sent to an incorrect recipient).

In recognition of the administrative drain that these obligations create for itself and CSPs, the ICO effectively disapplied them earlier this year by advising CSPs that it would not take enforcement action over failure to report low-risk incidents within 24 hours, so long as these incidents are notified within 72 hours of detection.2 We support the ICO's position as materially reducing the burden of these reporting obligations while still maintaining a high standard of protection for individuals through the GDPR's breach reporting rules. However, we note the uncertainty created by these obligations remaining in law while being disapplied in practice, so we therefore invite policymakers to formally remove these reporting requirements. This could be drafted as follows:

- Add a new clause to Part 4 of the Bill stating, 'Omit Regulation 5A (Personal data breach)'.

[2] https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2023/02/update-on-the-ico-s-change-of-approach-to-regulating-communication-service-providers/

Contact: Dani Dhiman, Policy Manager - Data
T 020 7331 2000 | E dani.dhiman@techuk.org

This removal received broad support from across industry and with government prior to publication and therefore we would hope that its removal would be uncomplicated and widely supported. We note that the draft ePrivacy Regulation looks likely to omit a specific reporting obligation for CSPs, which the Article 29 Working Party welcomed as "*prevent[ing] unnecessary overlap with the data breach requirements of the GDPR*".[3]

Digital Verification Services

The digital identity measures in the Bill will enable the Secretary of State to exercise governance functions in relation to the 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.

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.

AI and the Future of Work

Artificial Intelligence is a technology that has recently captured the public's imagination, but it is important to remember that AI as a technology is not good or bad by nature, and that responsible AI can unlock great benefits for society – in the workplace freeing us of some repetitive tasks for example.

The use of AI in the workplace needs to be appropriate, proportionate and, context-based with a strong ethical underpinning from the outset. Companies need to make sure that employees understand how AI is being used in their workplace or how their data is used, as studies have shown that employers are more likely to adopt the technology in a positive way if they are consulted. Equally, tech companies must ensure that there is a human in the loop to review AI processes with significant or legal effects and have clear lines of escalation for accountability and effective risk management purposes.

As the Government this year looks to set out its approach to governing AI, we must ensure that the UK's long-standing, deep-rooted expertise in digital ethics is at the heart of addressing any challenges associated with AI.

Use of Children's data

The UK GDPR contains provisions intended to enhance the protection of children's personal data and to ensure that children are addressed in plain clear language they can understand[4]. This remains untouched in the Bill, and organisations will maintain these obligations. Additionally, "safeguarding children" will be a new processing activity in the legitimate interest

[3] Page 7, WP 247, available at: https://ec.europa.eu/newsroom/article29/items/610140
[4] Children and the UK GDPR | ICO

Contact: Dani Dhiman, Policy Manager - Data
T 020 7331 2000 | E dani.dhiman@techuk.org

list no longer requiring a balancing test, which will reduce costs and time for businesses seeking to protect children's data rights.

Alongside this, we are engaging closely with the ICO on its guidance around content moderation and age assurance which will help businesses meet the requirements of the UK's new online safety laws. During this process, we urge the ICO to work in lockstep with Ofcom to ensure that guidance and support is coordinated, and businesses are clear on their responsibilities.

When techUK gave oral evidence to the Bill Committee on Wednesday 10 May the Member of Parliament Folkestone and Hythe, Damian Collins, asked:

"With regards to children's data rights, do you think the Bill will have any implications for the way in which the age-appropriate design code has been implemented by companies working within it now? It is not expressly written into the Bill, but do you expect there to be change?"

In response techUK set out that provisions in the Bill (relating to further processing) would likely provide greater clarity for businesses to process data to comply with the code. Further we remind the committee of the legitimate interest change above that will also improve business's ability to comply with the code by providing additional legal clarity and certainty around the processing of data for the purpose of safeguarding children.

The Member of Parliament Folkestone and Hythe asked for an example of where this might work in practice.

One envisaged example is in the processing of data to determine whether a service is likely to be accessed by a child to inform how a service might therefore seek to comply with the Age-Appropriate Design Code.

We believe both the change to the legitimate interest provisions outlined above as well as proposed changes to further processing would improve businesses' abilities to comply with the code.

Contact: Dani Dhiman, Policy Manager - Data
T 020 7331 2000 | E dani.dhiman@techuk.org