

DATA BILL WILL SET BACK UK ECONOMY AND RIGHTS

Briefing on the Data Protection and Digital Information Bill
April 2023

The Data Protection and Digital Information (DPDI) Bill will have its second reading in Parliament on April 17 2023, after months of delays, internal civil service confusion, and strong civil society opposition.

In an ever-digitalised and data-driven world, existing data protection laws provide much needed legal protection for the public against predatory commercial practices and the increased use of algorithmic decision-making across public services, law enforcement and employment.

The government has an opportunity to strengthen the UK's data protection regime post Brexit. However, it is instead setting the country on a dangerous path that undermines trust, furthers economic instability, and erodes fundamental rights.

The DPDI Bill will weaken your constituents' data protection rights, water down corporate accountability mechanisms, empower the Secretary of State with undemocratic controls over data protection, and negatively impact the economy. We highlight key concerns across these four areas:

Weakened data protection rights

New barriers to exercising data protection rights (Clause 7)

- Organisations can deny or charge a fee to individuals for the right to access information, the right to erasure and the right to object to processing if they decide these requests are "vexatious or excessive". This is vague, ill-defined and open to interpretation and will lead to more requests being refused. Charging a fee creates a barrier for many people, particularly those on lower incomes.

Lower protections around AI and automated decision-making (Clause 11)

- The Bill changes current rules that prevent companies and the government from making solely automated decisions about individuals that could have legal or other significant effects on their lives. Under proposals in the Bill, organisations will be able to use automated decision-making in these cases unless it is based on special category data (such as health data or political beliefs). It will also be more difficult to seek remedies or redress against unfair decisions (for example to challenge A-level grades or unfair dismissals).

It will take longer to resolve complaints (Clauses 8, 39, 40)

- The Information Commissioner's Office (ICO) will have the discretion to dismiss complaints, unless individuals have already complained to an organisation and company first.
- A new loophole will allow companies and organisations to reset the one month time limit for responding to individuals' requests (such as access to data or erasure) by asking further information.
- UK residents seeking justice against an infringement of their rights will have to wait longer for a rights' request to be processed and undergo a privatised complaint procedure with the offending organisation before being able to lodge a complaint with the ICO.
- The combination of these changes means that complaints could routinely take 20 months or longer to resolve.

Less public scrutiny and accountability

Weakened accountability framework (Clauses 14, 15, 17 and 18)

- The Bill removes requirements to keep Records of Processing Operations, Data Protection Impact Assessments, and Data Protection Officers, and replaces them with less robust requirements that only need be fulfilled in limited circumstances.
- The Bill also removes the requirement to consult with people affected by high risk data processing, thus making these assessments less reliable and objective.

Reduced accountability for businesses

- The Bill makes it easier for companies and organisations to circumvent legal data protection requirements by:
 - Misclassifying personal data as anonymous data (Clause 1);
 - Allowing personal data to be used for commercial purposes under the guise of "research purposes" (Clauses 2, 3 and 9);
 - Removing cookies' consent requirements for online tracking and personalised advertising (Clause 79).

Undemocratic expansion of government powers

Politicising the ICO (Clauses 28 and 31)

- The ICO plays a key role in the oversight of the government's handling of data so it is vital that it is completely independent from government. However, the Bill will give the Secretary of State new powers to issue instructions to the ICO and to interfere with how it functions. For instance, the government will be given the power to issue a statement of strategic priorities to the ICO and require the regulator to respond in writing as to how it will address them. Additionally, the ICO will have to seek the approval of the UK Government before issuing Codes of Practice.

Lowered protections for personal data transferred abroad (Schedule 5)

- The Secretary of State will be able to approve international transfers to countries with weak data protection and a lack of enforceable rights and effective remedies. In particular, the new "data protection test" for international transfers:
 - Does not have to consider the impact that foreign legal frameworks concerning defence, national security, criminal law and the access of public authorities to personal data, will have on the protection of UK personal data;
 - Does not require an independent and effective supervisory authority in the country where data is being transferred, or the availability of a judicial redress;
 - Gives arbitrary discretion to the UK government to consider, as a justification for authorising international data transfers, "any matter which the Secretary of State considers relevant".

Expanding government control over data (Clauses 5 and 6)

- The Secretary of State will be given additional powers to introduce (without meaningful democratic scrutiny) new grounds for processing data and new exemptions that would legitimise data uses regardless of the impact this may have on individuals. The list of exemptions is overly broad and vague. For instance, it includes "crime detection", "national security" or "disclosures to public authorities". The UK government is given broad powers to amend this list at any time and without meaningful limits to their discretion.

Negative impact on the UK's economy

Endangering EU adequacy

- The Bill will greatly weaken people's data protection rights and open new avenues for the UK to transfer data to countries with poor data protection, creating a scenario where the data of EU citizens could be laundered through the UK to countries that the EU does not have an agreement with. These changes are raising red flags in Europe and jeopardize the UK's current adequacy agreement. Conservative estimates found that the loss of the adequacy agreement would cost 1 to 1.6 billion pounds in legal fees alone.¹ This figure does not include the cost resulting from disruption of digital trade and investments.

Harming UK businesses

- Numerous businesses have spoken out about the negative impacts of the Bill's proposals.² Some startups are already fleeing the UK in anticipation of this reform.³ Navigating multiple data protection regimes will significantly increase costs and create bureaucratic headaches for businesses. Just as many businesses have adjusted to GDPR and put proper protocols into place, they will again be asked to adjust to a vastly different regime. Additionally, a separate data protection regime creates barriers between the UK and its closest trading partner.

For more information on this Bill, get in touch with

mariano@openrightsgroup.org and abigail@openrightsgroup.org.

About Open Rights Group (ORG): Founded in 2005, Open Rights Group (ORG) is a UK-based digital campaigning organisation working to protect individuals' rights to privacy and free speech online. . ORG has been following the UK government's proposed reforms to data protection since their inception. In June 2022, we organised an open letter signed by a coalition of over 30 organisations that highlighted the failure of the DCMS to properly engage with civil society groups about the proposed reforms, and in March 2023, we delivered a letter signed by 25 CSOs to Michelle Donelan, highlighting our serious concerns with the Government's draft legislation.

Imprint: Published by Open Rights, a non-profit company limited by Guarantee, registered in England and Wales no. 05581537. The Society of Authors, 24 Bedford Row, London, WC1R 4EH. (CC BY-SA 3.0).

1 See *The cost of data inadequacy* at: <https://neweconomics.org/2020/11/the-cost-of-data-inadequacy>

2 See, for instance, *15 CEOs of SaaS Companies open letter to Michelle Donelan*, at: https://www.linkedin.com/posts/adhale_data-protection-letter-to-secretary-of-state-activity-6992876772790784000-ztEB/

3 See *Back to the EU* at: <https://adambird.com/posts/back-to-eu/>