DATA BILL WILL SET BACK UK ECONOMY AND RIGHTS

Briefing on the Data Protection and Digital Information Bill

November 2023

The Data Protection and Digital Information (DPDI) Bill will have its report stage in Parliament on November 29 2023. In this briefing, we explain how the Bill weakens data rights (page 2), lowers scrutiny and accountability (page 3), unduly expands Government powers (page 3) and harms the UK economy and relations with the EU (page 4)

The Bill will weaken UK data protection rights, reduce accountability for private businesses and the Government, and have a negative impact on the UK economy: In an ever-digitalised and data-driven world, existing data protection laws provide 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 Bill will take away controls the public has over its data and hand more power to government bodies and corporations.

The Bill lowers standards and removes protections and redress mechanisms against harmful uses of artificial intelligence (AI): AI systems are built, trained, and sustained by access to the huge amount of of data that companies and governments collect about us. AI and automated-decision making systems have been found to replicate and amplify biases that exist in every day life. We need strong data rights protection to ensure that our data is not misused by AI systems.

The Bill will impact marginalised people, for whom data protection is extremely important: For example, refugees and asylum seekers, must share data with the authorities in order to apply to live in the UK. If, as proposed, their personal data could be more easily shared with their country of origin or with UK law enforcement or national security bodies, they could be at risk of persecution or harm. This may undermine their trust in the authorities and discourage them from seeking help or accessing needed services, such as healthcare, legal aid, or social support programs.

The Bill is set to undermine the UK adequacy decision, which allows the free flow of personal data from the EU to the UK and underpins important cooperation initiatives with the EU in trade, law enforcement and research. The loss of the adequacy agreement would cost UK businesses £1 to 1.6 billion in legal fees alone.[1] These are the risks the Government is taking in order to reduce their accountability and allow bad-faith companies to test dangerous technologies on your constituents.

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

Weakened data protection rights

New barriers to exercising data protection rights (Clause 8)

- **The Bill lowers the threshold that allows organisation to deny or charge for a data rights request**, such as to access or delete personal data, from manifestly excessive to "vexatious or excessive'. This term is open to interpretation and will lead to more requests being refused.

Lower protections around AI and automated decision-making (Clauses 8, 12)

- **Clause 8 would disempower individuals against false accusations of sexual assault[2] or bribery[3] made by AI applications.** The Bill will give organisations the right to refuse requests to erase or correct data if they lack resources to do so. AI systems are complex, designing them in a way that allows ex-post amendments is expensive.[4] However, AI is trained on data, and inaccurate data means AI and automated systems make mistakes.
- **Clause 12 removes the right to say no to automated decision-making.** Although individuals would retain a right to appeal automated decisions, this would be of little use, as individuals would lack access and resources to scrutinise and challenge how an AI system works.

It will take longer to obtain redress against injustices (Clauses 9, 41, 42)

- **Victims of data abuses will have to wait longer for a rights' request to be processed** and undergo a privatised complaint procedure with the offending organisation before lodging a complaint with the ICO. In turn, complaints could routinely take 20 months or longer to resolve.[5]
- Also, the Bill will expand the ICO's discretion to dismiss complaints, condoning rather than addressing their poor track record on handling complaints from the public.[6]

2 See *ChatGPT smeared me with false sexual harassment charges: law professor*, at: https://nypost.com/2023/04/07/chatgpt-falsely-accuses-law-professor-of-sexual-assault/

3 See *Australian mayor readies world's first defamation lawsuit over ChatGPT content*, at: https://www.reuters.com/technology/australian-mayor-readies-worlds-first-defamation-lawsuit-over-chatgpt-content-2023-04-05/

4 See *Algorithms that forget: Machine unlearning and the right to erasure*, at: https://www.sciencedirect.com/science/article/pii/S026736492300095X

5 See *Towards Making Systems Forget with Machine Unlearning*, at: https://ieeexplore.ieee.org/abstract/document/7163042

6 See David Erdos, University of Cambridge, *Towards Effective Supervisory Oversight? Analysing UK Regulatory Enforcement of Data Protection and Electronic Privacy Rights and the Government's Statutory Reform Plans*, at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4284602

Less public scrutiny and accountability

Weakened accountability framework (Clauses 15, 16, 18 and 19)

- **The Bill removes important accountability requirements**, such as 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 to 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.
- **The Bill threatens responsible AI governance by removing existing accountability rules.** It's important to have standardised documentation and practice for assessing risks throughout the AI lifecycle, ensuring effective enforcement by the ICO, and increasing overall transparency. However, the Bill removes "prescriptive requirements" of the UK GDPR, making this documentation less coherent, less useful and more prone to misrepresentation.

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 10); and
  - removing cookies' consent requirements for online tracking and personalised advertising (Clause 83).
- **These changes are particularly concerning for when seen in relation to the training of AI.** The DPDI Bill extends lower regulatory standards set forth by research provisions to "commercial research". However, research exemptions were meant to underpin public interest research, not the deployment of commercial products that will have practical implementations, which will impact people's lives.

Undemocratic expansion of government powers

Politicising the ICO (Clauses 29 and 30, 33)

- **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 the ICO with a statement of strategic priorities and require the regulator to respond in writing as to how it will address them. The ICO will also have to seek the approval of the Government before issuing Codes of Practice. 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.

Removing critical oversight of biometrics use and surveillance (Clauses 111, 112, 113)

- **The Bill abolishes the role of the Biometrics and Surveillance Camera Commissioner.** A report[7] by the Centre for Research into Surveillance and Privacy warns that, "plans to abolish and not replace existing safeguards in this crucial area will leave the UK without proper oversight just when advances in artificial intelligence and other technologies mean they are needed more than ever".

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" 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.

[7] See Gov.uk, *Changes to the functions of the BSCC: independent report*, at: https://www.gov.uk/government/publications/changes-to-the-functions-of-the-bscc-independent-report

Negative impact on the UK's economy and EU relations

Harming UK businesses

- **Numerous businesses have spoken out about the negative impacts of the Bill's proposals.**[8] Some startups are already leaving the UK in anticipation of this reform.[9] Navigating multiple data protection regimes will significantly increase costs and create bureaucratic headaches for businesses. A separate data protection regime creates barriers between the UK and its closest trading partner.

Undermining adequacy and threatening relationships with the EU

- **Loosing the UK adequacy decision would introduce significant frictions in trade, undermine the competitiveness of UK businesses, and threaten important relationships with the EU including law enforcement, research, and the Windsor Framework.** The European Commission issued in a written statement that the powers to the Secretary of State and proposed changes to the Information Commissioner's Office "raise questions with respect of the level of protection" for personal data in the UK.[10] Likewise, the European Parliament found that the Bill raises significant concerns over the implementation of the EU-UK Trade and Cooperation Agreement.[11] Several EU civil society groups have already demanded the UK Adequacy Decision be scrapped if this Bill is passed.[12]

For more information on this Bill, get in touch with mariano@openrightsgroup.org and james.baker@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.

8 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/

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

10 See *Answer given by Mr Reynders on behalf of the European Commission*, at: https://www.europarl.europa.eu/doceo/document/E-9-2023-001790-ASW_EN.html

11 See: *OPINION OF THE COMMITTEE ON CIVIL LIBERTIES, JUSTICE AND HOME AFFAIRS*, at: https://www.europarl.europa.eu/doceo/document/A-9-2023-0331_EN.html#_section11

12 See *Open Letter to the EU Commission regarding UK's data bill*, at: https://peoplevsbig.tech/open-letter-to-the-eu-commission-regarding-uk-s-data-bill