Data Protection and Digital Information Bill

Briefing note from CONNECTED BY DATA

- Data is a significant source of power in modern democratic societies. It is becoming fundamental to the social and political contract between citizens and the state, and to transactions between consumers and the private sector.
- The Data Protection and Digital Information Bill undermines existing safeguards and democratic governance of data and misses a critical opportunity to extend it for citizen, community, business and public benefit.
- Amendments are needed to: address the collective impacts and risks of modern data processing; empower those affected by automated decision making; and build trust through transparency, effective redress mechanisms, and public participation.

Background

Our lives have become digitised. Data about who we are, what we do and the environment we live and work in is collected about us constantly, whether we realise it or not. Whoever controls that data, be that big corporations or governments, has incredible power. They can use our data to do good – discover better treatments, target help to those who need it, fight climate change – but also exacerbate existing inequalities and cause terrible harm.

In modern data processing, organisations don't just use our data to make decisions about us individually. They pool our data together to analyse trends and predict behaviour. This ranges from Netflix recommendations, to predictions about prisoners reoffending. Data about us affects other people; their data affects how we are treated. And, as data reflects our history and not our desired future, it is often those in marginalised communities who are most vulnerable.

It's only by enabling people to build collective power to control how their data is collected, governed and managed that we can ensure data works for everyone. We are connected by data. Local communities, workers and other groups need to be given a meaningful say in data decisions so they can demand that data is used to build a just, equitable and sustainable world.

The Government has framed the Data Protection and Digital Information Bill (DPDIB) as delivering a 'Brexit benefit' through divergence from the EU GDPR: reducing compliance requirements on business and boosting innovation potential.

Brexit is an opportunity to adapt the UK's data laws to contemporary data processing and develop regulations that build on the UK's strengths. The Data Bill could enable, encourage and enforce the adoption of best-in-class, modern, data governance practices. However, as currently drafted it fails to do so, and in some cases it takes backward steps. It removes current controls and safeguards that protect UK citizens. It reduces opportunities for engagement that would encourage ethical and responsible uses of data, particularly for public good, and build public understanding and trust. It will damage public trust and undermine uses of data for the public good, while reducing the confidence of small businesses and charities to use data.

Targets for amendment

There are several areas of concern in the current Bill. Here we focus on ensuring the full set of **interests of those affected by data collection and use** are protected, to mitigate harms and retain trust while advancing the use of data, particularly for public benefit.

Data processing has collective impacts on groups and society

The Bill frames data protection as being about privacy. It isn't. This mistaken starting point means the Bill – like the GDPR and Data Protection Act (DPA) before it – fails to tackle the role of data in advancing other rights such as equality, education, or access to public services. Data regulation should advance our collective interests in strong democratic institutions, in a sustainable environment, and in economic growth and innovation. The Bill both increases the risk of data-driven harms and reduces the opportunities for data-related benefits.

Organisations make decisions about what and how data can be collected and used all the time. These decisions should always include consideration of the wider impacts of data on people, communities, society, equality, and the environment. Amendments are needed to embed meaningful consideration of collective and societal interests when:

- organisations carry out balancing tests for legitimate interest uses of data (Clause 5)
- the Secretary of State (SoS) creates new recognised legitimate interests (Clause 5)
- assessing the need for organisations to keep records of data processing (Clause 15)
- organisations carry out risk assessments (Clause 17)
- the ICO goes about its duties (Clause 27)
- the ICO creates codes of practice (Clause 29)
- the Secretary of State or Treasury require the provision of customer data (Clause 62)
- the Secretary of State or Treasury require the provision of business data (Clause 64)

Automated decision making affects people who aren't data subjects

Because it focuses on privacy and not impact, the Bill confuses who a decision affects with the source of the data used to make that decision. A decision made about you may have little to do with your data, and far more to do with data about other people you have never met. Regulating decisions made about people solely on the basis of data held about them will have limited, even counter-productive, effects.

The Bill needs to correct this. Amendments are needed to the Bill to properly protect the interests of decision subjects as follows:

- define decision subjects and give them rights arising from automated decision-making (Clause 11)
- consider decision subject rights and interests when the SoS creates new recognised legitimate interests (Clause 5)
- consider the impact on decision subjects when assessing the need for organisations to keep records of data processing (Clause 15)
- ensure codes of conduct consider decision subjects as well as data subjects (Clause 19)
- ensure the ICO protects the rights of decision subjects as well as data subjects (Clause 27)
- enable decision subjects to make complaints about automated decision-making (Clause 39)

Building trust requires transparency, accountability and participation

Recent uses of data by the government and corporations has led to a crisis of trust. The GP data grab led to millions of people withdrawing consent to use their health data for research. The Ofqual algorithm scandal led to people chanting "F**k the algorithm" on the streets. Surveys show only 30% of people trust the government to use data about them ethically, and only 5% trust big tech companies to do so (YouGov/ODI, 2019).

The Bill does nothing to remedy this situation and in several places makes it worse. It sweeps away checks and balances around the use of data around national security, crime, safeguarding and democratic engagement. It removes consultation with those affected by data collection and processing during the data protection risk assessment process.

Amendments are needed to the Bill to build trust around the use of data:

- scrap the ability of organisations to classify complaints as vexatious or excessive (Clause 7)
- reinstate and enhance consultation with data subjects (and wider stakeholders) during risk assessment processes (Clause 17)
- require the transparent publication of risk assessments and legitimate interest assessments, particularly by public authorities (Clause 17)
- enable organisations – such as unions or consumer rights bodies – to make complaints on behalf of data and/or decision subjects (Clause 39)
- remove the power to create "recognised legitimate interests" (Clause 5), or (if blocked) remove the list in the Bill (Schedule 1), pending proper consultation on their impact

About **CONNECTED** BY **DATA**

CONNECTED BY **DATA** is a campaign to give communities a powerful say in decisions about data to create a just, equitable and sustainable world. We want to put community at the centre of data narratives, practices and policies through collective, democratic and open data governance. We are a non-profit company limited by guarantee founded in March 2022 with funding from the Shuttleworth Foundation, and a staff team of three.

Our Executive Director, Dr Jeni Tennison OBE, is an internationally recognised data expert from her years of leadership at the Open Data Institute (ODI) and her role as co-chair of the Data Governance Working Group of the Global Partnership on AI. She is an associate researcher at the Bennett Institute for Public Policy at the University of Cambridge and an adjunct Professor at the Web Science Institute at the University of Southampton.