Data Use and Access Bill Public Bill Committee

Dear Chair and Committee Members,

Re: Data Use and Access Bill - Automated Decision-Making

We write with collective concern regarding the changes to automated decision-making safeguards in Part 5 of the Bill. Clause 80 of the Bill as drafted will severely undermine the keystone AI safeguard that protects people from automated decisions being made about them, without their choice or control.

The level of control and agency that people have over significant decisions made about their lives by AI will have a profound and lasting impact on public attitudes to these technologies, and the reforms in the Bill carry the severe risk of undermining public confidence in, and adoption of AI. This damage to public confidence will harm the government's overall growth mission and its goals for using technology to transform public services.

The use of automated decision-making is growing massively

Automated tools, including AI, are increasingly being used to make or support decisions that change the course of people's lives. Automation is already used to inform recruitment decisions, assess academic performance, and mediate access to financial loans and welfare services from banks and the public sector.

The current law provides a crucial baseline of protection against solely automated decision-making ('ADM'). The 'democratisation' of AI tools means that automated decision-making is being deployed at a much greater scale across the economy than ever before and into many more high-risk contexts with no sectoral regulation, like employment and recruitment contexts.

ADM protections have already proved crucial in protecting people

Previous regulatory interventions and documented incidents show the necessity of these legal protections, which safeguard against biased decisions and unfair power imbalances between algorithmic systems and data subjects. Deliveroo's use of the 'Frank' platform to manage more than 8,000 gig worker riders through ADM was found to be unlawful by the Italian Data Protection Authority, which held it 'produced a significant effect on the riders, consisting of the possibility of allowing (or refusing) access to job opportunities'. A Dutch court arbitrating a case brought by British claimants similarly ruled against Uber and Ola's opaque practices of automated decision-making. The scope of the ruling encompassed automated dismissals, automated pay setting, automated pay docking, and work performance profiling to determine how work is allocated among drivers – finding all of these practices unlawful. While data subjects found justice under GDPR in the Netherlands, where the data was controlled, these protections could be taken away from the same British workers under proposed changes to UK law.

The importance of retaining strong protections against automated decision-making will only increase. A recent audit conducted by the ICO found that *"AI is increasingly being used in the recruitment process to save time and money, helping to source potential candidates, summarise CVs and score applicants"*. The Government has expressed the intention to support the widespread adoption of AI tools by both public and private organisations, in a context where central departments like DWP have implemented algorithms that falsely flagged 200.000 people for fraudulent activity.

The Bill fundamentally alters when ADM is allowed, and the substitute protections are inadequate

The safeguards around automated-decision making - which exist only in data protection law - are therefore more critical than ever in ensuring that people understand when a significant decision about them is being automated, why that decision is made, and have routes to challenge it or ask for it to be decided by a human**.**

Concretely, the new Article 22 implemented by Clause 80 of the Bill has the following implications:

- **It removes individuals' choice and control over ADM** - Where currently ADM can only take place with a data subject's consent, under contract, or when explicitly legislated for, Clause 80 proposes to remove the broad prohibition on ADM. Where up until now people have had some degree of control over when ADM happens to them for significant decisions, it will now be up to data controllers to decide for example, whether they think it's in their legitimate interest to apply ADM to data subjects - meaning it can happen without their consent. This is a fundamental change that removes the ability to choose whether to be subject to ADM.

- **It places the enforcement burden on affected people, not those processing** - Removing the prohibition on ADM will place all the effort of preventing unlawful or unfair decision-making on the data subject. Individuals would in practice be required to scrutinise and contest decisions that are taken by systems that are outside of their reach or control. Their right to object to ADM under Article 22 can be overridden by the controller, with individuals having to prove that they have a right to object that prevails over the controller's interests. This is likely to be difficult in practice and effectively shifts the onus on the individual rather than the organisation deploying ADM.

- **The safeguards don't enable redress in practice:**
    - **People can't get enough information to appeal decisions** - Recent independent legal analysis commissioned by the Ada Lovelace Institute found that in reality, the type of information received by people about decisions that affect them was insufficient to mount a legal challenge: "[They] *lack legally mandated, meaningful, and in-context transparency that would alert individuals to the possible harm they face and allow them to evidence it*."

The current law only enables people to get general information about the logic of the system that made the decision – not a personalised explanation of why that decision was taken – and the Bill's safeguards do not improve the position. Without a personalised explanation, people cannot understand whether a decision was fair or discriminatory or reach the burden of proof necessary to overturn that decision in law.

- **'Human in the loop' safeguards only work if the human is empowered to review a decision** - a 2022 study of the implementation of these human-machine systems found humans in the loop experience "a diminished sense of control, responsibility, and moral agency." Human algorithmic moderators can lack technical capabilities or authority to influence decisions, which in turn create a false sense of security about the safety of ADM. To be in any way meaningful, human involvement or intervention must be by someone with sufficient authority and competence to review the decision. The Bill provides no definition of these terms.

- **The 'special category data' prohibition is narrower than it looks –** the Bill still prohibits automated decisions made on special categories of data such as health status or ethnic origin, but there are many kinds of data not included in this shortlist that it would be invasive, unfair or otherwise sensitive for decisions to be made on without a higher level of protection – for example, the Bill enables making automated decisions about people based on their socioeconomic status, regional/postcode data, inferences about their emotions, or even their regional accent - all with only the basic set of safeguards.

- **The safeguards can be removed at will -** The safeguards are easily removable for given decisions under secondary legislation. The Secretary of State powers under Clause 80 are so widely drawn that they would permit regulations to be laid that disapply the safeguards entirely to whole categories of processing (ie by declaring them not 'solely automated' or not a sufficiently 'significant decision'). There are no constraints on interpretation of these terms on the face of the Bill, so the meaning given to them in secondary legislation could be completely arbitrary. We urge Parliament to consider the level of power this will grant future governments to remove safeguards without meaningful parliamentary scrutiny.

- **Organisations won't be incentivised to implement the safeguards properly** - presently, an organisation looking at their data protection compliance is heavily incentivised to consider and document whether their processing will involve solely automated decision-making, and if so, how they will seek to meet one of the exceptions to the prohibition – for example by securing explicit consent from the person in question. This forces the organisation to engage critically with their practices around automated decision-making. In practice, under the Bill, the organisation is only incentivised to implement *some form* of the safeguards – the effectiveness of which will only become apparent much later in the deployment of a decision-making system, once decisions are being made about people's lives. The Bill does not specify what effective

compliance with the safeguards looks like or require any documentation of safeguard implementation that would incentivise early consideration of the safeguards by data controllers.

- **A code of practice cannot fill holes in the law** - Codes of practice are useful mechanisms for bringing clarity to the application of the law for both individuals and businesses and could ensure that controllers have more guidance on compliance expectations. But they cannot address most of the gaps described above; a code of practice for ADM will not mean people get to choose whether they are subject to ADM, that people get enough information to meaningfully appeal decisions made about them, and it will not make the safeguards less vulnerable to being removed.

- **Weakening people's rights in this way threatens UK-EU data adequacy -** the European Commission's decision that the UK provides an equivalent level of data protection is due to expire in June 2025. Weakening data protection rights in the UK risks a divergence from EU standards that may jeopardise cross-border flows, which would be of significant cost to the UK economy. The Northern Ireland Human Rights Commission has recently recognised this risk and the particularly detrimental effect it would have on the enjoyment of rights, such as access to all-island healthcare.

In summary, while the Bill may appear to provide greater clarity around ADM and its safeguards, in practice it fundamentally broadens the ability of controllers to conduct ADM and undermines the limited safeguards by specifying no expectations about their implementation and leaving it to the government to decide when and whether they should apply.

Public trust in AI and widespread disempowerment is at stake

The Secretary of State recently told Parliament in setting out his ambitions for AI adoption:

> *"Trust is incredibly important in this whole agenda. We have seen too many times in the past where a fearful public have failed to fully grasp the potential for innovation coming out of the scientific community in this country. We are not going to make that mistake. We understand from the outset that to take the public with us we must inspire confidence."*

ADM safeguards are critical to public trust in AI, and the cornerstone of how we embed automation into our lives. The public want more and better regulation of data and data-driven technologies. They rank *'clear procedures for appealing to a human against an AI decision'* as one of the most important things that would make them more comfortable with the use of AI.

The level of control and agency that people have over significant decisions made about their lives by AI will have a profound and lasting impact on public attitudes to these technologies. The lack of control many people will feel in the absence of meaningful safeguards will be a gift to anti-establishment sentiment that trades on such disempowerment.

This is one of the few decisions about the future of AI in our lives that is currently before Parliament. We urge the Committee to engage seriously with these concerns and secure ADM protections that will enable the UK to integrate these technologies responsibly and realise their opportunities with the benefit of sustained public confidence.

Sincerely,

Gaia Marcus, Director
Ada Lovelace Institute

Jasleen Chaggar, Legal and Policy Officer
Big Brother Watch

Rachel Coldicutt OBE, Founder
Careful Industries

Dr Jeni Tennison OBE, Executive Director
Connected by Data

Lord Bishop of Oxford, Rt. Rev. Steven Croft
Church of England

Jen Persson, Director
Defend Digital Me

Gavin Freeguard
Freelance

Dr. John Puntis, Co-Chair
Keep our NHS Public

James Killock, Executive Director
Open Rights Group

Caroline Wilson Palow, Legal Director
Privacy International

Professor Shannon Vallor, Co-Director, BRAID (Bridging Responsible AI Divides)
The University of Edinburgh

Professor Ewa Luger, Co-Director, BRAID (Bridging Responsible AI Divides)
The University of Edinburgh

James Farrar, Director
Worker Info Exchange

Public Law Project