The Data Protection and Digital Information Bill: A threat to fair markets and open public services

BRIEFING PAPER

March 2024

By Alex Lawrence-Archer and Ravi Naik, AWO

The Data Protection and Digital Information Bill, currently at Committee stage in the House of Lords, is set to undermine vital rights that protect vulnerable consumers and help workers understand how they are monitored by companies and public bodies. The Bill is a threat to fair markets and open public services.

KEY POINTS

- The government is seeking to fundamentally alter the UK's data protection regime through a Bill reforming the UK GDPR.
- As well as threatening the UK's 'data adequacy' determination from the EU (which allows data to freely flow between the UK and EU), it undermines crucial rights:
  - It will be easier for organisations to ignore requests and take longer to resolve disputes, creating an incentive to refuse the exercise of data subject rights.
  - Processing in many areas – such as the excessive data collection on gig economy workers to detect supposed fraud – will be easier.
  - A new definition of personal data may drastically reduce protections for 'pseudonymised' data, including that processed by third party processors often used by sectors such as the gambling industry.
- Vulnerable workers and consumers have come to rely on these rights:
  - Gig economy workers use data rights to understand how platforms regulate their participation in rigged markets, giving them greater bargaining power.
  - Online gambling customers have uncovered how companies profile them to maximise profits, even when they have stopped gambling.

RECOMMENDATIONS

- The new 'recognised legitimate interests' should be removed, retaining the requirement to consider how data processing affects individuals.
- The new and lower thresholds to refuse data subject requests should be removed.
- The new definition of personal data must be clarified.
- Representative bodies should be empowered to bring claims and 'super-complaints' on behalf of data subjects to improve levels of legal compliance.

FOREWORD

By Lord Clement Jones CBE

This briefing paper emphasizes how the Data Protection and Digital Information Bill currently going through Parliament dilutes data subjects' rights and increases the compliance complexities for businesses operating in both the UK and the European Union.

Key concerns include the redefinition of "personal data," the introduction of new "legitimate interests" for data processing without consent, and the potential undermining of the Information Commissioner's Office (ICO) independence. The Bill introduces the concept of "recognised legitimate interest," eliminating the need for a balancing test in certain scenarios, which is seen as a step back from current data protection standards.

Changes to Subject Access Requests (SARs) are also being made. The threshold for refusing SARs is being lowered, and businesses may classify more requests as "vexatious," potentially impacting individuals' ability to access data held about them.

The Bill's approach to automated decision-making is alarming too. It reframes the right to human intervention in AI decisions but shifts the responsibility for ensuring legality from the decision-maker to the affected individual, potentially reducing safeguards and transparency.

The Bill proposes changes to international data transfers, introducing a more flexible, risk-based approach to adequacy decisions. This has significant implications for maintaining data protection levels and the longevity of the EU's adequacy decision.

There are also concerns about the Bill's lack of comprehensive AI regulation, oversight of biometrics, and safeguarding against the misuse of AI-generated content, such as child sexual abuse material (CSAM).

Rather than dilution of data subject rights we need a stronger focus on collective data rights, more robust safeguards for automated decision-making, and regulatory frameworks that ensure transparency and accountability in AI systems.

This is an extremely useful and authoritative briefing paper. It makes it clear that the Bill is a significant step back from current data protection standards, potentially compromising individuals' privacy rights, introducing ambiguity, and risking the UK's data adequacy status with the EU, which could have profound implications for businesses and trade. There is no Brexit dividend to be found here.

FOREWORD

By Dr Ann Kristin Glenster, Executive Director, The Glenlead Centre and Senior Policy Advisor on Technology and Governance Law, Minderoo Centre for Technology and Democracy at the University of Cambridge

Highly technical and often misunderstood, the current UK data protection regime guarantees all individuals some fundamental rights in regard to their personal data. It forms the cornerstone for how we are treated as digital citizens in the automated world driven by surveillance capitalism. Data protection is finely calibrated to protect the fundamental rights and interests of individuals and at the same time enable the free flow of data. By ensuring that personal data is processed in an accountable and fair manner, data protection also enables innovation and stimulates growth.

As this briefing rightly sets out, the Data Protection and Digital Information Bill will undermine those objectives. As the authors discuss, the proposed changes will make it harder for individuals to exercise their rights. Changes to the definition of personal data will limit the scope of the law in ways that are incommensurate with technical advances whereby new forms of data emerge as categories of personal data. Changes to the legal basis of legitimate interest means that individuals may have to justify why they wish to exercise a fundamental right. Individuals who are already struggling to assert their rights will find it harder, more expensive, and in many cases futile to claim protection for their personal data.

The effects will be stark. The power imbalance between individuals and large data controllers, especially Big Tech and public services, will widen drastically. The knock-on effect will not only be felt by individuals; business too will suffer. As this briefing aptly points out, uncertainty about definitions and legal obligations introduced in this Bill are likely to add 'red tape' and increase the compliance burden considerably. These changes will disproportionately affect small-to-medium businesses more than large corporations, thus allowing for data hoarding to continue to flow to the top. The result is likely to be industrial capture of data which will determine the path for innovation, and thus the potential for economic growth, in the UK in ways that will have a radical impact on our future.

Data protection was meant to guarantee fundamental rights that could not be sold or bartered away. The Data Protection and Digital Information Bill does just that. To avoid this scenario – and the impact it will have on the UK's data protection regime's EU adequacy status – Parliament should adopt the recommendations herein. While the Bill's proposed changes may seem to only introduce a few technical alterations, their likely effect if adopted without the changes proposed in this briefing, will be profound.

In an age of artificial intelligence, where our world is shaped by algorithms, data processing, and automation, British citizens and businesses need all the protection and advantages they can get. This Bill does not do that. The result will instead be a continued favouring of foreign tech providers to hoard, generate, use, and create personal data in ways that will shape our economy and shape our lives. This Briefing Paper sets out a few targeted recommendations that would return data protection to is intended purpose of protecting individuals' rights and freedoms while allowing the economy to thrive.

THE UK GDPR EMPOWERS AND PROTECTS INDIVIDUALS

Data rights

It is a common misconception that the UK General Data Protection Regulation (GDPR) primarily relates to the placement of 'cookie banners' on websites[i]. In fact, the data protection framework protects individual citizens and consumers by placing limits on how organisations can analyse and profile (and therefore influence) them.

Perhaps most importantly, the UK GDPR gives people important rights that allow them to understand – and make choices about – how they are being monitored and profiled[ii].

These include:

- The right to access copies of the information an organisation holds about you;
- The right to object to certain types of processing, such as information used to market products or services to you;
- The right to have your personal data erased when it is no longer relevant or has been processed unlawfully.

A tool for workers and consumers to redress power imbalances

Real-world examples exist that demonstrate the positive impact the UK GDPR has made on ordinary people's lives.

For example, research has shown that gambling companies systematically monitor and profile their customers, calculating the profit available if self-excluded gamblers are 'won back' into gambling, and targeting them with personalised special offers and emails at their most susceptible moments.[1]

In 2021, the user of an online gambling website used GDPR rights to lay bare the complex architecture of monitoring that gambling platforms had used to build detailed profiles of his behaviour and his addiction. His story attracted coverage in both the national and international press[2], exposing the previously unknown scale and intensity of profiling by the gambling industry, including a system of 'win-back' profits from offering special offers to customers who had stopped gambling.

[i] In fact, such banners are part of compliance with the Privacy and Electronic Communications Regulations (2006) and are a form of 'compliance theatre' in that if online services made real efforts to comply with the law, such banners would be unnecessary.

[ii] The UK GDPR places an emphasis on the purpose for which personal data is processed. This means that – when properly enforced – it can and does protect data subjects like online gamblers from exploitative processing, while permitting the same data to be processed for other purposes, such as problem gambling checks.

Similarly, workers in the gig economy have been using data rights to uncover how digital platforms tip the scales in their favour in the markets that they control.[3] This information is being used by workers to collectively organise and slowly regain some bargaining power. Over four million precarious and low-paid workers are active in the gig economy in the UK, and research shows that in recent years algorithmic management has been moving into 'higher status' sectors and affecting white collar workers too.[4] In 2023, a group of UK gig economy workers used their GDPR rights to secure judgments reversing their 'robo-firing' from the platforms they worked for. [5]

Both of these examples show how those who are most vulnerable to monitoring and profiling have been using GDPR data rights to redress the power imbalances they face when companies and public bodies influence their lives through data processing. Individuals have also used data rights to understand and challenge how public bodies monitor them by building up profiles of their political views based on social media activity with a view to excluding them from events.[6] Revealing these practices has helped to make policymaking more open and transparent.

A THREAT TO DATA RIGHTS

The Bill as currently drafted poses a serious threat to people's data rights – and by extension to fair markets and open public services.

Scope of the GDPR's protection set to narrow

Clause 1 of the Bill creates a new definition of 'personal data'. In doing so, it changes a fundamental concept that underpins the UK's data protection regime. The new definition requires data to be protected as 'personal' only where it is 'likely' that individuals may be identified from it. This is narrower than the current definition and could lead to more instances in which individuals are identified from '*anonymous*' datasets by unscrupulous operators and hostile actors.

A good illustration of this would be a pseudonymous dataset which by itself does not enable individuals to be identified but does so when combined with information from another source (e.g. through a hack or leak). Currently, that data would be protected. Under the new definition, it would only be protected if identification is 'likely'. If a leak or hack is not likely but merely possible, or a risk to guard against, then the data will not fall within the scope of the UK GDPR's protection.

This creates a paradoxical situation in which organisations are not obliged to protect such data despite the very real risk of data breaches that could lead to identification of individuals. This change is relevant in many fields where pseudonymous data is used, such as the health sector and where companies track individuals' internet use, creating a considerable risk of privacy breaches including in relation to sensitive data.

Data rights to be limited

New test for refusing data subjects' requests

Clause 9 of the Bill will allow controllers to refuse the exercise of data subject rights – including the right to access or to object to processing – where the request is interpreted to be 'vexatious or excessive'. This replaces the current test in the UK GDPR under which requests can only be refused in cases when they are deemed 'manifestly unfounded or excessive'. The Bill then lists a wide range of vague factors to be taken into account in determining whether it is vexatious or excessive, including 'the nature of the request' and 'the relationship between the data subject and the controller'. It is unclear what these phrases mean or how they are to be weighed.

For example, it is unclear if a closer relationship between a data subject and data controller would mean that a request is more likely to be deemed "vexatious". If so, this interpretation could have a deleterious impact on, for example, employees seeking to understand how their data has been used. Controllers may be able to demand that data subjects provide reasons for exercising their data rights – something not permitted under the current regime. Allowing controllers to ask for the intention of the request could be intimidating for individuals.

Lower standard of search in response to requests for access to data

A recent amendment to the Bill further weakens the right of access, considerably limiting the search that organisations should carry out in response to a request for access to data. This raises the prospect of organisations refusing to be transparent to those they monitor on the basis that it is 'too complex' to query their own systems in response to a request.

Delays in resolving simple complaints

Finally, the Bill introduces new and longer timeframes for dealing with individuals' requests. The practical effect – in combination with the likely increase in satellite complaints about the right of access – is that many standard complaints will take 20 months or longer to resolve.

In many cases, such a delay would defeat the purpose of the rights entirely. Consider, for example, an employee who wishes to know how they are being surveilled in the workplace. In 20 months they may well have moved on, defeating their right to understand how they are being monitored by their employer. Even in the best case scenario, these longer delays will place a huge administrative burden on ordinary people who are simply seeking to exercise their legal rights.

At best, this change will cause delay and increase opportunities for controllers to tie data subjects up in lengthy correspondence or force collateral litigation. At worst, it could lead to a considerable reduction in the extent to which people understand – and can control – how they are tracked and profiled by large organisations who find the idea of being open about their processing uncomfortable. It is especially those organisations with the greatest incentives to refuse data subject rights whose processing needs to be brought into the open by the exercise of those rights.

New scope for organisations to carry out intrusive processing

Legal basis for processing

Under the UK GDPR, any processing of personal data requires an applicable 'legal basis'. While this might be the individual's consent (the basis with which people are most familiar), organisations can also process personal data when it is in their 'legitimate interests' to do so, subject to the vital caveat that they must consider the impact of their activities on the individuals affected and must not proceed if to do so would be unfair.

A new automatic gateway for processing

Clause 5 of the Bill creates a new legal basis for processing personal data known as 'recognised legitimate interests'. This will make data processing automatically lawful when a controller deems it 'necessary' according to a list of vaguely-defined purposes such as 'preventing crime' or 'democratic engagement'. Unlike the current rules, the Bill proposes to remove the requirement to consider how an organisation's activity might affect individuals.

This departs from a longstanding and fundamental principle of data protection: the principle that the impact of a process on individuals matters and that organisations must openly explain why their processing is justified. It is likely to lead to a significant expansion in excessive monitoring and profiling where organisations can stretch these vague definitions to meet their purposes.

For example:

- Gig economy platforms will be more able to justify their scrutiny of workers' movements partly on the basis of the need to prevent and detect 'fraud';
- Private stores will find it easier to use intrusive facial recognition monitoring, scanning thousands of customers each day, in order to reduce petty crime and loss margins;[7]
- Political candidates will likely seek to define more of their activities as 'democratic engagement', which includes opinion polling by contractors working under their authority, in order to segment people's views and micro-target them through monitoring their online activity.

Limited benefits for businesses

The Bill has been justified on the basis of bringing benefits to businesses.[8] In fact, many of these benefits – at least to SMEs – are doubtful, since any business doing business with Europe will need to either (i) reorganise their business and compliance systems to comply with two very similar but slightly divergent regimes, or (ii) simply continue complying with the higher EU standard of data protection.

THE NEED FOR SCRUTINY AND AMENDMENT

A rushed process

The Bill has been rushed through its Parliamentary stages. Prior to its readings in the Lords, the Government introduced 150 pages of last-minute substantive amendments at Report Stage in the Commons.[9] It is essential that Parliament is given time to scrutinise these amendments.

The regulation of data processing is fundamental to how our economy and society work now and into the future. Only by striking the right balance can legislators ensure fair markets and open public services.

Recommendations

We therefore recommend:

- The new 'recognised legitimate interests' should be removed, retaining the requirement to consider how data processing affects individuals.
- The new and lower thresholds to refuse data subject requests should be removed from the Bill.
- The new definition of personal data must be clarified to reduce the risk of hacks and leaks leading to privacy breaches.
- Representative bodies should be empowered to bring claims and 'super-complaints' on behalf of data subjects to improve low levels of legal compliance.

None of these amendments would place new limits on controllers' access to data where their processing is for the *benefit* of data subjects. Rather, they address the exploitation of personal data for organisations' own purposes.

This briefing sets out only a few examples of how the Bill will hollow out rights and protections for UK citizens. Parliamentarians must be given adequate time to scrutinise the changes in this Bill and propose and debate amendments which ensure that the UK retains the standard of data protection that its citizens and markets need.

ENDNOTES

[1] https://cleanupgambling.com/news/clean-up-gambling-submits-evidence-to-ico-on-data-abuse

[2] https://www.bbc.co.uk/news/technology-56580411

[3] https://www.workerinfoexchange.org/research

[4] https://joint-research-centre.ec.europa.eu/system/files/2021-05/jrc124874.pdf

[5] https://www.adcu.org.uk/news-posts/uber-to-reinstate-robo-fired-drivers-and-pay-compensation

[6] https://www.theguardian.com/education/2023/sep/30/revealed-uk-government-keeping-files-on-education-critics-social-media-activity

[7] https://www.awo.agency/latest/big-brother-watch-complaint-against-private-sector-facial-recognition/

[8] https://www.gov.uk/government/news/changes-to-data-protection-laws-to-unlock-post-brexit-opportunity

[9] https://x.com/HansardSociety/status/1731236941650182225?s=20