Data (Use and Access) Bill: Automated decision-making in the spotlight

Proposals grant controllers increased flexibility for automated decision-making, provided suitable safeguards are implemented. By **Fiona Maclean**, **Gail Crawford**, **Amy Smyth** and **Lorenzo Meusburge**r of Latham & Watkins.

On 23 October 2024, the UK government introduced the Data (Use and Access) Bill (the Bill) to Parliament, marking a significant step in the evolution of the country's data protection landscape. It follows previous reform attempts that lapsed after the July 2024 government change. The proposed legislation aims to reform various aspects of UK data protection law while also addressing broader initiatives related to data access and digital identity. Among its many provisions (138 Clauses, 16 Schedules and 251 pages to be precise), the Bill outlines notable changes in the realm of automated decision-making. In this article, we will delve deeper into the Bill, with a particular focus on the legislative changes surrounding automated decision-making, exploring their potential implications and the future they may herald for individuals and organisations alike.

Overview of the Bill

Compared to the previous government's flagship data protection reform initiative (the Data Protection and Digital Information (No. 2) Bill), the current Bill proposes slightly less extensive changes to the current data protection regime, but retains a number of the earlier proposals, such as those on legitimate interests, automated decision-making, and ICO reforms. Key proposals include:

1. Enhanced access frameworks for customer and business data, which will make it more efficient for both industry and the public to use personal information in beneficial ways and which mirror certain provisions in the EU's Data Act;
2. A framework for individual ID verification services;
3. Targeted amendments to UK data protection law, maintaining the UK GDPR framework but with changes including:
   a) a specific list of "recognised legitimate interests", which are exempt from the UK GDPR's balancing test for the purposes of the legitimate interest legal basis;
   b) a relaxation of the current restrictions on automated decision-making ;
   c) a risk-based approach to adequacy decisions (rather than the EU's equivalence-based approach), which will be applied by the Secretary of State, and which will require third countries to maintain protections "not materially lower" than those in the UK;
   d) a less restrictive approach to cookies and tracking technologies, in particular allowing certain non-intrusive cookies and similar technologies without user consent and enabling consent via browser tools to reduce the use of consent banners. Additionally, it proposes increasing fines for breaches of the cookie-related rules in the Privacy and Electronic Communications Regulations 2003 to UK GDPR levels, i.e. up to £17.5 million or 4% of global turnover; and
4. Transitioning the ICO to a new corporate structure, renamed the 'Information Commission'.

The Bill is currently going through the legislative stages and is subject to further debate and amendment. It has passed its first and second readings in the House of Lords as well as the Committee stage, and at the time of writing was at the Report stage.

What are the proposed changes to ADM?

Currently, under Article 22(1) of the UK GDPR, individuals have the right to not be subjected to decisions made solely by automated processes, including profiling, that have legal effects or similarly affect the individual, unless (i) where such processing is necessary for entering into, or the performance of, a contract between a controller and a data subject, (ii) where such activity is required or authorised by law[1], or (iii) where a data subject has provided explicit consent (Article 22(2)).

Clause 80 of the Bill introduces notable changes to the existing framework under Article 22 UK GDPR. Specifically, the Bill substitutes Article 22 with new Articles 22A-D whereby unrestricted automated decision-making is not limited to those three circumstances described above. In essence, the Bill's changes mean that, apart from cases using special category data, automated decision-making, which results in a legal or similarly significant effect, will no longer be restricted (and permitted only under those three lawful grounds described above), but instead, such processing will be permissible regardless of the lawful basis relied on, as long as suitable safeguards are in place. The ICO, in its commentary on the Bill, notes "[m]ost significantly, this will now allow organisations to rely upon legitimate interests for this type of processing".[2]

The Bill's aim with these changes is to provide more flexibility to businesses while retaining appropriate assurances and safeguards for data subjects (which are discussed in more detail below). In the ICO's response to the Bill, the Information Commissioner welcomed the proposed changes

introduced by the Bill with respect to Article 22 UK GDPR, and stated: "In my view, this strikes a good balance between facilitating the benefits of automation and maintaining additional protection for special category data."[3]

Does the Bill alter the definition of ADM?

The proposed new Article 22A of the UK GDPR defines automated decision-making and retains the existing elements under Article 22 UK GDPR, although it supplements it with the element of "meaningful human involvement". Specifically, it states that "a decision is based solely on automated processing if there is no meaningful human involvement in the taking of the decision, and a decision is significant, in relation to a data subject, if (i) it produces a legal effect for the data subject, or (ii) it has a similarly significant effect for the data subject" (Article 22A(1)).[4] Articles 22D(1) and D(2) confer powers to the Secretary of State to clarify what qualifies as (i) meaningful human involvement, and (ii) a significant decision with similarly significant effect for the data subject. The explanatory notes to the Bill state that these powers "will allow the Secretary of State to determine when meaningful involvement can be said to have taken place in light of constantly emerging technologies, as well as changing societal expectations of what constitutes a significant decision in a data protection context."

Until such regulations have been published by the Secretary of State, organisations may want to consider existing guidance which is helpful in respect of certain interpretive matters. For example:

- According to the ICO's guidance on the term "solely"[5], if a human inputs the data or merely applies the decision taken by the machine, the process would still be considered a solely automated decision made by an automated system. However, if a human actively evaluates and interprets the automated decision before it is applied to an individual, the process would not be considered solely automated, so long as such action is more than a mere token gesture and the human reviewer has real discretion to alter the machine's outcome. One could reasonably presume that the new element of "meaningful human involvement" will rely and build on this existing guidance.
- A decision with a legal effect impacts a person's legal status or rights, such as eligibility for a legal benefit like housing assistance. A decision with a similarly significant effect has a comparable impact on an individual's circumstances, behaviour, or choices. The assessment here should be contextual, meaning that similarly significant effects may arise with respect to the treatment of vulnerable individuals (like children), but may not arise in other circumstances. Examples include automatic denial of online credit, e-recruitment without human involvement, discrimination and exclusion of individuals, and relevant factors to consider include the impact on a person's financial situation, health, reputation, employment opportunities, behaviour, or choices.

In addition, note that under the new Article 22A(2), "when considering whether there is meaningful human involvement in the taking of a decision, a person must consider, among other things, the extent to which the decision is reached by means of profiling." It is currently unclear what the profiling element (i.e. that controllers need to consider the extent to which the decision is reached based on profiling) means in practice, and what impact such element has on a controller's assessment whether there is meaningful human involvement. Neither the explanatory comments to the Bill, nor the ICO's technical drafting comments provide additional clarity.

In conclusion, Article 22A does not propose any radical departure or material changes to the meaning of automated decisions and the proposed changes mostly bring the law in line with what existing ICO guidance has already stated, although there is no doubt that the publication of supplementary regulations by the Secretary of State under Article 22D(1) and D(2) (as well as regulatory guidance on the profiling element described above) will be welcomed by individuals and businesses for additional certainty.

What are the limitations on the new ADM provisions?

The proposed language for the new Article 22B(1) makes clear that a "significant decision" (i.e. one that produces legal effects or in a similar way significantly affects the data subject) may not be taken by a controller on the basis of automated decision-making, if it is entirely or partly based on the processing of special categories of data (as set out Article 9(1) UK GDPR).[6] In such case, lawful processing requires controllers to meet one of the following two conditions:

1. The controller obtains the data subject's explicit consent; or
2. The processing is necessary for reasons of substantial public interest (per Article 9(2)(g) UK GDPR) and the decision is either:
   a) necessary for entering into, or performance of, a contract between the data subject and a data controller; or
   b) required or authorised by law.

A further notable restriction introduced by the Bill is that where processing of, or on behalf of, the decision-maker is based on new Article 6(1)(ea) of the UK GDPR (i.e. processing is necessary for the purpose of a recognised legitimate interest), then a significant decision solely based on automated processing may not be taken.[7]

Implications for controllers' use of AI systems

The Bill's proposed changes will simplify a number of processing operations that may have previously required careful planning and comprehensive risk assessments in order to comply with Article 22 UK GDPR. For example, in the realm of AI processing, the proposed relaxations will be beneficial to businesses who want to deploy AI tools on datasets containing non-special categories of personal data for automated decision-making. This aligns with the UK's general principles-based approach to AI regulation, which is currently relatively light-touch and seeks to facilitate innovation by affording businesses with more flexibility around automated decision-making (in particular when deciding on the extent of human review within the automated decision-making process). Although a

limitation on the processing of special category data for automated decision-making persists, the new framework encourages responsible innovation, as long as certain safeguards, such as transparency and review processes, as explained below, are upheld by the controller. Below are two use cases where the legislative proposal may benefit controllers:

- **In HR and recruitment**, AI tools can streamline decisions, such as on the calculation of wages, bonuses, or decisions regarding access to employment benefits, dismissals, etc. as well as assist with the initial screening of job applications by filtering candidates based on predefined criteria. Under the current requirements, there is a risk that the aforementioned use cases could fall within the scope of Article 22 UK GDPR (depending on the particular circumstances) and controllers may therefore find themselves restricted with what tools they can implement to make decisions about individuals, as an appropriate legal basis may not be available. The proposed changes mean that controllers will have more flexibility with respect to the legal bases they deem most appropriate to the processing (unless the processing includes special categories of personal data), though they will still need to implement the proposed safeguards outlined below (including on the provision of human intervention on the data subject's request), and comply with other generally applicable provisions of the UK GDPR for the processing of personal data. In practice, controllers should review any AI-generated outcomes that may materially affect employees and job candidates to ensure that no individual is disadvantaged, for example, as a result of algorithmic biases.
- **In the financial services sector**, automated systems are often used for credit scoring and loan approvals. Using such automated systems, for example for credit scoring to determine loan approvals, will likely fall within the scope of Article 22. However, under the proposed changes in the new framework, such use case would no longer be restricted to the three specific legal bases permitted under Article 22(2) (unless controllers use special categories of personal data) and businesses could undertake automated decision-making using AI to process applications more swiftly by relying on a legitimate interest legal basis (depending on the specific circumstances). Controllers would, however, still need to comply with other applicable GDPR provisions for such processing (including a balancing test), and implement appropriate safeguards (as detailed below), including reviewing mechanisms for identifying cases that fall outside standard parameters (e.g. with respect of vulnerable individuals), to ensure that applicants are not, for example, unfairly denied credit.

To what extent does the Bill diverge from the EU GDPR?

The proposed UK approach to automated decision-making under the Bill appears to somewhat diverge from the expansive interpretation of Article 22 EU GDPR, as seen in the recent SCHUFA decision by the Court of Justice of the EU (C-634/21) (*PL&B International Report*, April 2024, p.1). In *SCHUFA*, the court applied Article 22 strictly, potentially extending its restrictions to data processing activities that precede the actual decision if the decision heavily relies on such processing.

This interpretation could, for example, bring a wide range of AI data analytics tools within the scope of Article 22 EU GDPR, impacting how businesses in the EU approach automated decision-making. In contrast, the UK's proposed framework under the Bill offers more flexibility by narrowing the scope of Article 22 UK GDPR.

This divergence could lead to notable differences in how automated decision-making is regulated and practised between the UK and EU, depending on how national courts and supervisory authorities choose to enforce the SCHUFA ruling. Businesses operating across both jurisdictions will need to navigate these differences carefully to ensure compliance.

What safeguards should controllers adopt for ADM?

The safeguards proposed by the Bill at Article 22C replace the current provisions at Article 22(3) and Article 22(3A) of the UK GDPR and s.14 of the Data Protection Act 2018. Any processing of personal data (including special category of data) will need to implement certain safeguards under the proposed new Article 22C, which provides that where a significant decision is taken by or on behalf of the controller in relation to a data subject and such decision is "(a) based entirely or partly on personal data, and (b) based solely on automated processing, the controller must ensure that safeguards for the data subject's rights, freedoms and legitimate interests are in place."

These safeguards must comply with any future regulations issued by the Secretary of State on automated decision-making, and must also consist of or include measures which:

a) provide the data subject with information about the significant decisions taken on the basis of automated means and associated personal data processing;
b) enable the data subject to make representations about such decisions;
c) enable the data subject to obtain human intervention on the part of the controller in relation to such decisions; and
d) enable the data subject to contest such decisions.

Practical implementation checklist

To implement the safeguards outlined in the proposed new Article 22C, controllers should focus on (i) transparency, (ii) human oversight, and (iii) effective communication. This involves:

1. Creating clear channels to inform data subjects about automated decision-making processes, including revising sufficiency of disclosures in existing privacy notices and update them, if necessary, to ensure they explain the personal data used and the logic behind decisions.
2. Establishing a dedicated team or allocating specific responsibilities to employees for oversight ensures that human intervention is available when needed, allowing for

meaningful human evaluation and the ability to alter outcomes if necessary.

3. Additionally, controllers should consider providing simple means in apps and sites for data subjects, possibly within existing account settings and data management tools, to submit feedback and request human intervention on any automated decision-making processes to engage with any decisions that may affect them.
4. In general, controllers should also consider regular audits and reviews of automated systems to identify potential biases or errors within the automated decision-making systems as well as the processing of any special category of data (for example on an incidental basis) to ensure compliance, fairness and accuracy.
5. Training staff on the legal and ethical implications of automated decision-making reinforces a culture of responsibility, while comprehensive policies and procedures of processes and decisions support transparency and accountability.
6. Concrete steps for controllers include documenting:
   a) the steps they have taken with regard to the above and the safeguards that have been implemented;
   b) the data used, decision criteria, and instances of human intervention within the automated decision-making process; and
   c) any changes made to decisions following data subject representations or human review.

Conclusion

There is no doubt that the Bill presents both challenges and opportunities for businesses. By embracing the flexibility offered by the new framework, companies can innovate responsibly, leveraging AI and automated decision-making to enhance efficiency and competitiveness. However, this must be balanced with a commitment to transparency and accountability, ensuring that the rights and interests of individuals are safeguarded. The Bill's emphasis on meaningful human intervention and robust safeguards underscores the importance of integrating human oversight into automated processes. For businesses, this means not only complying with legal requirements but also fostering trust *vis-a-vis* their data subjects.

For the moment, the Bill's reception by trade unionists, civil society groups, and academics has been rather negative, as seen in an open letter dated 6 December 2024[8] to Technology Minister, the Rt Hon. Peter Kyle, urging amendments to the Bill to change its proposals on automated decision-making. The campaigners caution that deviating from existing data protection laws could strip individuals of their right to avoid "life-changing decisions made solely by machines." Signatories, including Amnesty International, Privacy International, and the Open Rights Group, advocate for revisions to the Data (Use and Access) Bill to maintain the accountability necessary for public confidence in AI technology and decisions solely made by machines.

AUTHORS

Fiona Maclean and Gail Crawford are Partners at Latham & Watkins, Amy Smyth is a Knowledge Management Counsel, and Lorenzo Meusburger is an Associate at the same firm.
Emails: fiona.maclean@lw.com
gail.crawford@lw.com,
amy.smyth@lw.com
lorenzo.meusburger@lw.com

REFERENCES

1 Note that in the UK GDPR, this exception refers to "qualifying significant decision" for the purposes of Section 14 of the 2018 Act). "Qualifying significant decision" is a decision taken by the controller that (i) produces legal effects or similarly significantly affects the data subject, (ii) is "required or authorised by law", and (iii) which does not fall within Article 22(2)(a) or (c) of the UK GDPR (i.e. decisions necessary to a contract or made with the data subject's consent). (Section 14(3) Data Protection Act 2018).
2 Available at: ico.org.uk/about-the-ico/the-data-use-and-access-dua-bill/information-commissioner-s-response-to-the-data-use-and-access-bill/
3 Available at: ico.org.uk/about-the-ico/the-data-use-and-access-dua-bill/information-commissioner-s-response-to-the-data-use-and-access-bill/
4 Note that the Bill seems to propose a slightly different approach for intelligence services' processing for automated decision-making under Part 4 of the Data Protection Act 2018. The Bill's Article 22D notes in this regard that "a decision is based on entirely automated processing if the decision-making process does not include an opportunity for a human being to accept, reject or influence the decision." According to the ICO's technical drafting comments at Annex One of the ICO's response to the proposed Bill, the aforementioned language resulted in a point of criticism as a result of the uncertainty with respect to what "opportunity" means. Specifically, the ICO notes that its understanding "is that the government's intention is that a mere 'opportunity' for human involvement in a decision will not be sufficient to take a decision outside of the scope of "a decision based on entirely automated processing". [Intelligence Services] Organisations would have to exercise this opportunity to have this effect. It would be useful to make the intent clear in the drafting or the explanatory notes."
5 Available at: ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/automated-decision-making-and-profiling/what-does-the-uk-gdpr-say-about-automated-decision-making-and-profiling/
6 Special categories of data include personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. (Article 9(1) UK GDPR)
7 Article 22B(4) Data (Use and Access) Bill
8 Available at: www.openrightsgroup.org/press-releases/letter-to-peter-kyle-keep-our-right-not-to-be-subjected-to-decisions-based-solely-on-ai/

ESTABLISHED 1987

UNITED KINGDOM REPORT

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

UK and EU – Cookie rules to become the 'law of everything'?

Greg Palmer and **Ceyhun Necati Pehlivan** of Linklaters analyse the proposed changes to cookie provisions in the UK's new Data (Use and Access) Bill, and the approach taken recently by the EDPB.

Helen Dixon, the former Irish Data Protection Commissioner famously described the GDPR as the "law of everything". The broad scope of the concepts of "processing" and "personal data" means almost everything any business does is subject to the GDPR.

Recent developments risk a similarly expansive application of the cookie rules. The UK's Data (Use

Continued on p.3

The ICO's consultation on generative AI: Key take-aways

The ICO expects the industry to significantly improve how it informs individuals about data processing. By **Josephine Jay** and **Annabel Loose** of Goodwin.

As the predominance of generative artificial intelligence (AI) continues to gather pace, legislators and advisory bodies face the challenge of fitting this technology into existing and emerging legal frameworks, without stifling innovation. Amongst other things, the large-scale data processing driving generative AI raises complex questions regarding compliance with data protection laws, including the

Continued on p.6

Issue 137 **JANUARY 2025**

UNITED KINGDOM
report

ISSUE NO 137 **JANUARY 2025**

PUBLISHER
Stewart H Dresner
stewart.dresner@privacylaws.com

EDITOR
Laura Linkomies
laura.linkomies@privacylaws.com

DEPUTY EDITOR
Tom Cooper
tom.cooper@privacylaws.com

REPORT SUBSCRIPTIONS
K'an Thomas
kan@privacylaws.com

CONTRIBUTORS
Greg Palmer and Ceyhun Necati Pehlivan
Linklaters

Josephine Jay and Annabel Loose
Goodwin

Fiona Maclean, Gail Crawford, Amy Smyth and Lorenzo Meusburger
Latham & Watkins

Rachael Annear, Joseph Mason, Adam Gillert and Rhea Dennis
Freshfields

Nicola Fulford
Hogan Lovells

Ralph O'Brien
REINBO Consulting

Lauren Reid
The Privacy Pro

PUBLISHED BY
Privacy Laws & Business, 2nd Floor,
Monument House, 215 Marsh Road, Pinner,
Middlesex HA5 5NE, United Kingdom
Tel: +44 (0)20 8868 9200
Email: info@privacylaws.com
Website: www.privacylaws.com
Subscriptions: The *Privacy Laws & Business* United Kingdom Report is produced six times a year and is available on an annual subscription basis only. Subscription details are at the back of this report.
Whilst every care is taken to provide accurate information, the publishers cannot accept liability for errors or omissions or for any advice given.
Design by ProCreative +44 (0)845 3003753
Printed by Rapidity Communications Ltd +44 (0)20 7689 8686
ISSN 2047-1479

comment

DUAB may make life easier for business

The new Data (Use and Access) Bill continues its passage through Parliament with the Report stage in the House of Lords on 21 and 28 January. In this issue our contributors look in more detail into four areas where there are some novelties; cookies (p.1), automated decision-making (p.12), digital identities (p.17) and international data transfers (p.16).

Some aspects of the Bill will be welcomed by DPOs such as the legitimate interest grounds for direct marketing, or narrowing SAR searches to what is "reasonable and proportionate". It is also reassuring that there will be no changes to the DPO role, rejecting the proposals in the previous Bill.

But there are also open questions about the interpretation of some of the Bill's wording, as was evident at the Bill Briefing event organised by *PL&B* with Linklaters (p.9). It may be that much of this work is left to the ICO in terms of issuing guidance. One area which generated a lively discussion was the new definition of "scientific research". While the Bill makes this concept wider it is still not clear what can reasonably be described as "scientific". Does the research need to be for public good? Or peer reviewed?

The Bill also establishes further protections for children by placing an additional statutory duty on the ICO to consider children's vulnerability regarding data processing. Children's privacy was also at centre stage at the global DPAs' assembly in Jersey in October last year (p.26).

PL&B is organising a one-day conference in London on 11 March on protecting children's privacy. As a subscriber benefit, you can get a free place at this event with speakers from the ICO, Lego, K-ID and Ontario's Information and Privacy Commissioner. You may register your interest now at info@privacylaws.com. Further details to come soon at www.privacylaws.com/children2025.

Laura Linkomies, Editor
PRIVACY LAWS & BUSINESS

Contribute to PL&B reports

Do you wish to contribute to *PL&B UK Report*? Please contact Laura Linkomies, Editor (tel: +44 (0)20 8868 9200 or email: laura.linkomies@privacylaws.com) to discuss your idea, or offer to be interviewed about your organisation's data protection/Freedom of Information work.

Join the Privacy Laws & Business community

The *PL&B United Kingdom Report*, published six times a year, covers the Data Protection Act 2018, the Freedom of Information Act 2000, Environmental Information Regulations 2004, Privacy and Electronic Communications Regulations 2003 and related legislation.

PL&B's United Kingdom Report will help you to:

Stay informed of data protection legislative developments.

Learn from others' experience through case studies and analysis.

Incorporate compliance solutions into your business strategy.

Learn about future government/ICO plans.

Understand laws, regulations, court and tribunal decisions and what they will mean to you.

Be alert to privacy and data protection law issues and tech developments that will affect your compliance and your reputation.

Included in your subscription:

1. Six issues published annually

2. Online search by keyword
Search for the most relevant content from all *PL&B* publications.

3. Electronic Versions
We will email you the PDF edition which you can also access in online format via the *PL&B* website.

4. Paper version also available
Postal charges apply outside the UK.

5. News Updates
Additional email updates keep you regularly informed of the latest developments.

6. Back Issues
Access all *PL&B UK Report* back issues.

7. Events Documentation
Access *PL&B* events documentation, except for the Annual International Conferences in July, Cambridge.

8. Helpline Enquiry Service
Contact the *PL&B* team with questions such as the current status of legislation, and sources for specific texts. This service does not offer legal advice or provide consultancy.

9. Free place at a *PL&B* event
A free place at a *PL&B* organised event when booked at least 10 days in advance. Excludes the Annual Conference. More than one free place with Multiple and Enterprise subscriptions.

privacylaws.com/reports

"The UK and International *PL&B* Reports have been my 'go to' resource for 20 years despite the wide choice of alternate resources now available."

Derek Wynne , SVP Privacy & Chief Privacy Officer, Paysafe

International Report

Privacy Laws & Business also publishes *PL&B International Report*, the world's longest running international privacy laws publication, now in its 37th year. Comprehensive global news, currently on 180+ countries, legal analysis, management guidance and corporate case studies on privacy and data protection, written by expert contributors

Read in more than 50 countries by regulators, managers, lawyers, and academics.

Subscriptions

Subscription licences are available:

- Single use
- Multiple use
- Enterprise basis
- Introductory two and three years discounted options

Full subscription information is at privacylaws.com/subscribe

Satisfaction Guarantee

If you are dissatisfied with the *Report* in any way, the unexpired portion of your subscription will be repaid.