Policy briefing – Data (Use and Access) Bill: Committee Stage

This briefing was prepared by the Ada Lovelace Institute ahead of Committee Stage for the Data (Use and Access) Bill (DUA Bill) on 4 March 2025. It covers the following topics:

For more information on any of the information contained in this briefing, please contact Ada's Associate Director (Law and Policy) at mbirtwistle@adalovelaceinstitute.org .

About the Ada Lovelace Institute

The Ada Lovelace Institute is an independent research institute with a mission to make data and AI work for people and society. This means making sure that the opportunities, benefits and privileges generated by data and AI are justly and equitably distributed.

Summary

The Data (Use and Access) Bill (DUA Bill) is a critical opportunity to build public and business confidence in data-driven innovation, acknowledging the central role it plays across the economy and civic life. Clear, comprehensive data protection law gives businesses the legal certainty they need, and safeguards fundamental rights such as privacy.

To realise the benefits of artificial intelligence (AI) – as articulated in the Government's AI Opportunities Action Plan - strong data protection will be critical.[1] Far from this being a purely technical Bill, **data protection law contains some of the only meaningful protections for individuals in current UK law from harms arising from the development and use of AI** - for example, how companies can lawfully use people's data for the training of AI systems, and how people are subject to decision-making informed by AI systems.

Whilst the Bill's retention of many of the UK GDPR's safeguards and individual data rights is commendable, its **provisions were first prepared over two years ago for a previous Bill – before the advent of general-purpose AI systems like ChatGPT ('GPAI')**

Ada is concerned that the impact of the proposed changes have not been fully considered in light of the last two years of AI development - namely:

- the 'democratisation' of AI tools that means that **automated decision-making is being deployed at 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.
- the economic incentives for large technology companies to acquire as much data as possible to train GPAI systems with is driving **compliance behaviour that deliberately pushes and exploits the boundaries of the law** around legitimate interests, scientific research, and data reuse – making it critical that these provisions leave no scope for abuse.

These trends mean it is critical to re-evaluate the safeguards for protecting personal data. Public attitudes around data use and access are complex and context-dependent – but research consistently demonstrates that the public expects appropriate regulation of their data and information about how it will be used,[2] and expresses concern about lack of agency when it comes to their data - supporting the need for credible data protection.[3]

[1] UK Government, Department for Science, Innovation and Technology (2025) *AI Opportunities Action Plan.*

[2] UK Government, Department for Science, Innovation and Technology (2023) CDEI publishes research on AI governance

[3] Ada Lovelace Institute (2022) *Who cares what the public think?*

The Bill contains some measures that would lower safeguards for personal data or in practice mean that data protection is much harder to enforce - in the process **risking public trust in data-driven technologies that is difficult to earn, and even more difficult to repair when harms occur**.

Ada has identified three aspects of the Bill that require particular parliamentary scrutiny:

1. **Automated decision-making.** The Bill removes the general prohibition on automated decision-making. This means that people no longer get to choose whether to be subject to automated decision-making, and places responsibility on them to enforce their rights rather than on companies to demonstrate why automation is permissible. Even with new safeguards being introduced, people will not get **meaningful explanations** about decisions that affect their lives and therefore be able to appeal them.

2. **Research provisions.** A key underlying policy priority for the Bill is to stimulate innovation, through broadening definitions of scientific research for which data can be shared and reused. As currently written, we believe these provisions are susceptible to misuse that would enable mass reuse of personal data scraped from the internet or acquired through social media for AI product development, under the auspices of 'scientific research' – with the potential for considerable public backlash.

3. **Regulation-making powers for the Secretary of State** which would enable the effective removal of key data protection safeguards via secondary legislation by adding 'recognised legitimate interests' that would allow organisations to bypass the core tests they otherwise need to comply with, to use people's data.

We urge parliamentarians to consider how the powers outlined in this Bill may be used by future governments. We propose a series of amendments below that aim to prevent potential abuses by providing additional protections and clarifications in the face of the law, ensuring that protections are not weakened or removed through secondary legislation.

1. Automated decision-making

Overview

Solely automated decisions (often referred to as 'automated decision-making' or 'ADM') are increasingly being used to make decisions on things that change the course of people's lives. ADM 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 'democratisation' of AI tools means that automated decision-making is being deployed at much greater scale across the economy than ever before and into many more high-risk contexts lacking sectoral regulation, like employment and recruitment contexts.

If and when generative AI-enabled 'assistants' take on decision-making roles currently delivered by those working across commercial and public services, for example, replacing therapists, personal companions, lawyers or financial advisors, and civil servants,[4] the impacts of ADM will become unprecedentedly more complex and prevalent.

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 that the decision be delegated to a human decision-maker**.**

In current law, Article 22 of the UK GDPR prohibits solely automated decision-making about individuals when that decision will have 'legal or similarly significant' effects. Unless the individual has given explicit consent or narrow legal exemptions apply, there must be a "human-in-the-loop" to review significant decisions by algorithms. Organisations must regularly review these systems to ensure that they make fair decisions, and individuals must be given an avenue to challenge decisions.

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. For example, 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'. [5] A Dutch court similarly ruled against Uber and Ola's opaque practices of automated decision-making and work performance profiling to determine how work is allocated among drivers.[6]

Implementing appropriate safeguards on ADM is also critical to ensuring public trust in 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. Our nationally representative survey of the British public found that 50% of respondents would like clear procedures in place for appealing to a human against an AI decision, while a similar proportion (54%) said they wanted 'clear explanations of how AI works'.[7] Research also shows having a human-in the-loop increases uptake of algorithmic systems, with

[4] Ada Lovelace Institute (2024) AI assistants

[5] The Future of Privacy Forum (2020) *Automated Decision-Making Under the GDPR: Practical Cases from Courts and Data Protection Authorities*

[6] Worker Info Exchange (2023) '*Historic digital rights win for WIE and the ADCU over Uber and Ola at Amsterdam Court of Appeal*'

[7] Ada Lovelace Institute (2024) It's time to strengthen data protection law for the AI era

one study finding doing so made participants 7% more likely to support the use of ADM.[8] The safeguards and provisions within Article 22 of the UK GDPR are central to ensuring public trust in AI systems.

When looking at the amendments to ADM safeguards, **it's crucial to understand how they will be implemented in practice; as organisations treat compliance with a prohibition very differently to a blanket 'permission with safeguards'.**

What the Bill says

Clause 80: Automated decision-making sets out substantial reforms for ADM. In current law, under Article 22 of the UK GDPR, solely automated decision-making is prohibited in all but three circumstances: where entering into a contract; or authorised by law; or with the explicit consent of the data subject). The proposed reforms remove these protections, and permit solely automated decisions as long as individuals affected by those decisions can make representations, ask for meaningful human intervention, and challenge decisions made by ADM. These rights for data subjects are set out under a new Article 22C.

Restrictions on ADM would however still apply where a decision relies on the processing of special category data, has a potentially significant "adverse legal effect", and is made without meaningful human involvement. In this scenario, decisions made by solely automated means would be permitted only with the individual's explicit consent, or where the decision is necessitated by a contract with that individual, or where the decision is required by law and there is a "substantial public interest" in the decision being made.

Lastly, the Secretary of State (SoS) is also given new regulation-making powers to determine "*when meaningful involvement [in relation to ADM] 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*."[9] In effect, this could give government scope to waive restrictions where novel data-driven technologies cannot practicably be influenced by a human in the loop, or where doing so simply undermines desired performance.[10]

Proposed Amendments

Clause 80 – Automated Decision-making

Amendment 1 – Clarifying what constitutes 'meaningful human involvement' in ADM

Amendment text:

Clause 80 - Section 4A, Article 22A – Automated processing and significant decisions

Page 95, line 19, add:

"3. For the purposes of paragraph 1(a):

a. a human is a natural person with the necessary competence and authority to understand and alter the decision."

[8] Sele, D.; Chugunova, M. (2022) Putting a Human in the Loop: Increasing Uptake, but Decreasing Accuracy of Automated Decision-Making

[9] https://www.gov.uk/government/publications/data-use-and-access-bill-factsheets

[10] A Feb 2024 study found putting a Human in the Loop for automated decisions can increase uptake, but generally decreases accuracy. Source: Sele, D.; Chugunova, M. (2022) Putting a Human in the Loop: Increasing Uptake, but Decreasing Accuracy of Automated Decision-Making

Explanation: This amendment provides some clarification of what is meant by ‘meaningful human involvement’ stipulated in 1(a). Specifically, that human reviewers of algorithmic decisions must have adequate capabilities, training, and authority to challenge and rectify automated decisions.

Amendment 2 – Restricting regulation making powers from Secretary of State

Amendment text:

Clause 80 – Section 4A, Article 22C - Safeguards for automated decision-making

Page 96, line 11, after “the controller must ensure that safeguards for the data subject’s rights, freedoms and legitimate interests are in place which comply with paragraph 2” ... delete:

“and any regulations under Article 22D(3).”

Explanation: Amendment 8 suggests amending Article 22D(3) such that this reference becomes moot. See Amendment 8 for more information.

Amendment 3 – Notifying individuals when ADM is involved in decision-making

Amendment text:

Clause 80 – Section 4A, Article 22C - Safeguards for automated decision-making

Page 96, line 12, add:

“(a) communicate to the data subject before and after the decision is taken the fact that automated decision-making is involved in the decision, the extent of any human involvement, and the availability of safeguards under this Article”

Explanation: This amendment places an obligation on the data controller to be transparent about when/how ADM are being used as a decision is being made. Organisations must notify individuals when automated decision-making tools are involved in decisions. as individuals cannot exercise their rights to representation and contest if they do not know that ADM are being used in the first place.

Amendment 4 – Providing individuals with personalised explanations

Amendment text:

Clause 80 – Section 4A, Article 22C -Safeguards for automated decision-making

Page 96, line 14, after “provide the data subject with information about decisions described in paragraph 1 taken in relation to the data subject” insert:

“...including meaningful information about the logic involved, the significance and the envisaged consequences of such processing for the data subject, and a personalised explanation for the decision”.

Explanation: 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. Independent legal analysis has found that the type of information received by people about decisions that affect them is insufficient to mount a legal challenge. This amendment introduces a requirement for a personalised explanation, so that people can understand decisions and meaningfully challenge them when needed.

Amendment 5 – Defining "personalised explanation"

Amendment text:

Clause 80 – Section 4A, Article 22C -Safeguards for automated decision-making

Page 96, line 19, add:

"3. For the purposes of paragraph 2(a), a personalised explanation must—

(a) be clear, concise and in plain language of the data subject's choice in a readily available format;

(b) be understandable, and assume limited technical knowledge of algorithmic systems;

(c) address how the decision affects the individual personally, explaining which aspects of the individual's data have likely influenced the automated decisions, or alternatively a counterfactual of what change in their data would have resulted in a more favourable outcome;

(d) be available free of charge and conveniently accessible to the data subject, free of deceptive design patterns."

Explanation: This amendment introduces a safeguard that clarifies what is meant by "personalised explanation" in 2(a), to ensure that these explanations help individuals to understand whether a decision was fair or discriminatory, and challenge or appeal this decision if needed.

Amendment 6 – Ensuring timeliness in data controllers' implementation of the safeguards

Amendment text:

Clause 80 – Section 4A, Article 22C -Safeguards for automated decision-making

Page 96, line 19, add:

"4. Where the safeguards apply after a decision is made, the controller must give effect to data subject requests as soon as reasonably practicable and within one month of the request."

Explanation: This amendment outlines a timeframe, within with organisations must respond to individuals who are exercising their right to representation or contest a decision. Without this clarification, organisations could take months or years to respond to individuals who are challenging or appealing a decision, rendering this safeguard insufficient and ineffective.

Amendment 7 – Adding a requirement for documentation of the safeguards

Amendment text:

Clause 80 – Section 4A, Article 22C - Safeguards for automated decision-making

Page 96, line 19, add:

"5. The controller must ensure the safeguards are fully in place and complete a data protection impact assessment under Article 35 before a decision under Article 22A is taken, documenting the implementation of the safeguards in addition to the requirements of that Article.

6. The controller must publish details of their implementation of the safeguards and how data subjects can make use of them."

Explanation: The addition of (5) introduces a requirement for documentation of safeguard implementation as part of an organisation's data protection impact assessment, to better incentivise early considerations of the safeguards by data controllers. The amendment will force organisations to engage critically with their practices around automated decision-making before these systems are deployed, so that the basic protections will always be effectively implemented.

The addition of (6) introduces a requirement on data controllers to be transparent around their use of ADM. Elsewhere in the Bill there are provisions for compelling controllers to proactively publish user-facing guidance on aspects of data protection (eg as in Clause 75). This thinking should also be applied to ADM, where controllers should be compelled to notify users where and how ADM is being used and provide information around their rights so they can understand how they are affected and make effective representations to the controller.

Amendment 8 – Restrict regulation making powers for the Secretary of State, with regards to defining "Meaningful human involvement" and "Similarly significant effect"

Amendment text:

Clause 80 – Section 4A, Article 22D – Further Provision about automated decision-making

Page 96, line 22, remove points (1) and (2).

Explanation: This amendment removes regulation making power for the Secretary of State, with regards to defining "meaningful human involvement" and "similarly significant effect". The addition of these powers, in effect, this could give this, or any future government scope to waive restrictions where novel data-driven technologies cannot practicably be influenced by a human in the loop, or where doing so simply undermines desired performance. This amendment, along with Amendment 9, proposes transferring these powers to the data protection regulator, who should be tasked with producing guidance to define key legal terminology in the Bill.

Amendment 9 – Task the Information Commissioner's Office with publishing guidance on what is meant by "meaningful human involvement" and "similarly significant effect"

Amendment text:

Clause 80 – Section 4A, Article 22D – Further provision about automated decision-making

Page 97, line 3, add:

"(2) The Commissioner must prepare and publish guidance on the application of Articles 22 A-D and related sections of GDPR and the Data Protection Act 2018 within six months of this Act coming into force and update it from time to time or at the request of the Secretary of State, including:

a. for the purposes of Article 22A(1)(a), the interpretation of meaningful human involvement in the taking of a decision, including non-exhaustive examples

b. for the purposes of Article 22A(1)(b)(ii), the interpretation of where a decision is, or is not, to be taken to have a similarly significant effect for the data subject, including non-exhaustive examples."

Explanation: This amendment shifts powers and responsibility for providing further legal clarification of "meaningful human involvement" and "similarly significant effect", from the Secretary of State to the Information Commissioner's Office. The ICO - through industry engagement, regulatory investigations, and its technology horizon scanning and public research functions – is best placed to provide evidence-based guidance on how emerging technologies and societal shifts impact the feasibility and necessity of including humans-in-the-loop for ADM.

2. Research provisions

Overview

Under current law, data that has been collected for one purpose cannot be reused for another purpose except in certain circumstances. This is a core component of how data protection law functions; **it makes sure organisations only use personal data for the reason it was collected**.

One of these exceptional circumstances is 'for scientific research'. Political attention on the definitions and uses of data within research increased in the wake of the COVID-19 pandemic, where some hold the view that legal uncertainty and related risk aversion were a barrier to clinical research.[11] There is a legitimate government desire to ensure valuable research does not have to be discarded because of a lack of clarity around data reuse, or because of very narrow distinctions between the original and new purpose.

The government position is that the Bill only clarifies the law, incorporating recitals to the original GDPR into the face of the legislation. While this may be the policy intention, **the Bill must be read in the context of recent developments in artificial intelligence and the practice of AI developers**.

The current generations of general-purpose AI systems like ChatGPT require the use of vast datasets, often scraped from the internet. The development of such models is often positioned as a scientific endeavour by their developers and may be supported by the production of academic papers. The line between product development and scientific research is blurred because of how little is understood about these new technologies. Many developers posit efforts to increase model capabilities, efficiency, or indeed the study of their risks as scientific research.

The economic incentives for large technology companies to acquire as much data as possible to train GPAI systems is driving **compliance behaviour that deliberately pushes and exploits the boundaries of the law** around legitimate interests, scientific research, and data reuse – **making it critical that these provisions leave no scope for abuse.**

The proposed definition of scientific research is too broad and will permit abuse for commercial interests, outside of the policy intention. The Bill must recognise the reality that *any AI development* will likely be positioned by companies to "reasonably be described as scientific" and combined with the inclusion of 'commercial activities' in the Bill opens the door to data reuse for **any data-driven product development** under the auspices that this represents 'scientific research' - even where their relationship to real scientific progress is unclear or tenuous. While we understand the policy intention of the definition to not include 'product development', this exclusion is not on the face of the Bill, and we urge Parliament to describe what commercial activities should not be considered 'scientific research'.

Moreover, large tech companies could abuse the provisions to legitimise mass data scraping. Personal data scraped from the internet or collected via 'legitimate interest' (eg by a social media platform about its users) could potentially be legally re-used for training AI systems under the new provisions, if developers can claim that it constitutes 'scientific research'. This kind of re-use has been previously attempted, most recently in Meta's controversial decision to use Instagram user data to train its AI models[12], triggering an ICO response because of the difficulty users encountered in objecting to such use.[13] **The move caused considerable public concern, including statements from celebrities opposing the use of such data without**

[11] Lalova-Spinks et al (2022) Challenges related to data protection in clinical research before and during the COVID-19 pandemic: An exploratory study

[12] Which (2024), *Facebook and Instagram plans to use UK posts to train AI models*

[13] Information Commissioner's Office (2024), *Statement in response to Meta's plans to train generative AI with user data*

consent.[14] However, if this kind of reuse is justified under the research provisions, this would **leave data subjects unable to object to such re-use, and probably unaware it was occurring.**

People may not even be told their data is being re-used - Clause 77 will mean personal data collected through mass scraping or ingested during AI training would not be subject to normal notification requirements if it involved 'disproportionate effort'. While these provisions have primarily been designed to enable old medical research to be re-used where research participants may no longer be contactable or alive, they could also be used by AI developers to argue that contacting people whose data has been scraped or ingested by an AI model during training is impractical, as training datasets are very large and unstructured and retrieving personal data stored in a trained AI model is technically challenging. **Data subjects cannot make use of their data rights if they do not even know their data is being processed**.

Beyond data protection, there is significant evidence of **innovation exemptions being systematically abused.** For example, this can be observed in the UK's experiences with R&D tax credits; HM Revenue and Customs' 2024 annual report revealed that the estimated cost of fraud and error in their Research and Development tax relief scheme was more than £4.1bn from 2020-21 to 2023-24. Commenting on the scheme in the media, taxation expert Colin Hailey stated *"[the tax relief scheme] was the wild west. These advisers were cold-calling firms and saying, 'you don't think you're doing R&D, but we can help you'.*[15]

Ada is concerned that the provisions could **be abused by organisations (particularly AI developers) to enable data re-use** <u>**at scale**</u> **in contradiction to the expectations and intentions of data subjects,** risking growth in public backlash to AI use. The research provisions should be tightened to better specify what re-use is intended and acceptable.

What the Bill says

Clause 67: Meaning of research and statistical purposes, and ***Clause 68: Consent to processing for the purposes of scientific research*** collectively intend to make it easier to comply with data protection law when conducting scientific research and broaden how this research is defined.

Clause 67 amends Article 4 of the UK GDPR to define what constitutes processing for scientific research under the UK GDPR and clarifies that it doesn't matter whether research is privately or publicly funded to meet this definition. New Article 4(4)(a) also gives non-exhaustive examples of the types of scientific research that could fall under the definition - including "*processing for the purposes of technological development or demonstration…so far as those activities can reasonably be described as scientific*". Article 4(4)(b) clarifies that research into public health only falls under the definition of scientific research if it is in the public interest.

Clause 68 clarifies how organisations conducting scientific research can gain consent to process data even where it is not possible to fully identify how this data will ultimately inform research outputs. In this scenario (which could for example apply where data is gathered in development of an AI model whose potential capabilities are not yet clear) consent must be consistent with 'generally recognised ethical standards relevant to the area of research", and data subjects are able to consent to only part of the research.

Clause 85: Safeguards for processing for research etc purposes outlines specific protections that should be afforded to data being used for scientific research. These safeguards include technical and organisational measures to ensure data minimisation, and the use of 'research ethics committee' and a 'body appointed for

[14] iNews (2024), *The 'Goodbye Meta AI' viral instagram hoax explained – and how to actually opt out*

[15] The Guardian (2024) 'Free money': £4bn lost to fraud and error on flagship HMRC 'innovation' scheme

the purpose of assessing the ethics' for medical research. This does not however seem to foresee 'ethics committees' for general scientific research, including commercial R&D.

Clause 77: Information to be provided to data subjects creates an exemption for notifying data subjects about how their data will be used in research, when there would be a "disproportionate effort" to provide this information. New paragraph 6 of Article 13 provides a non-exhaustive list of factors for the controller to determine what constitutes a "disproportionate effort" - including the number of data subjects, the age of the personal data and any appropriate safeguards applied to the processing.

Amendment passed during House of Lords Committee Stage

Clause 67 - Meaning of research and statistical purposes

Ensuring scientific research making use of the reuse exception is in the public interest

Amendment text:

Clause 67

Page 75, line 10, after "scientific" insert "and that is conducted in the public interest"

Explanation: This amendment ensures that to qualify for the scientific research exception for data reuse, that research must be in the public interest. This requirement already exists in the Bill for medical research but should apply to all scientific research wishing to take advantage of the exception.

- **Summary:** The following amendment was passed in the House of Lords. It amendment ensures that any scientific research making use of the exception for data reuse must be in the public interest. This is not a new requirement, but a clarification that reflects the intention of the original GDPR.

- **Rationale:** 'Public interest' is a key characteristic of genuine scientific research - for example, in advancing academic knowledge in a given field. It is also an established term under UK GDPR, and the subject of ICO guidance.[16] As a test, it ensures that processing activity must have some public interest purpose or outcome beyond any benefits to the data controller.

- ***Legal Scrutiny* -** The government's claim that adding a public interest test will place a significant additional burden on scientists and researchers *does not bear out*. A public interest test considers whether research will increase the stock of knowledge – including knowledge of humankind, culture and society – and/or devise new applications of available knowledge.[17] **Adding a public interest test will not introduce an undue bureaucratic burden on researchers, as the vast majority of scientific research in academic domains will meet this test**, where there is an intention to increase the amount of publicly available knowledge **-** as even a discounted hypothesis from a failed experiment does so. The recitals to the original GDPR frame scientific research purposes with the expectation of

[16] Information Commissioner's Office, *UK GDPR Guidance and Resources: The Research Provisions – Principles and grounds for processing*

[17] OECD (2015) Frascati Manual: Guidelines for Collecting and Reporting Data on Research and Experimental Development

a public interest outcomes, e.g., reuse under consent should be in line with “legitimate expectations of society for an increase of knowledge should be taken into consideration” (Recital 113). This expectation of some kind of public interest being served for scientific research provisions to apply is also reflected in European jurisprudence; the European Data Protection Supervisor issued a preliminary opinion on research provisions under GDPR, which maintains that “*the special data protection regime for scientific research is understood to apply where each of the three criteria are met … (3) the research is carried out with the aim of growing society’s collective knowledge and wellbeing, as opposed to serving primarily one or several private interests*”. [18] Departure from this understanding in what is permitted under the Bill would likely influence the UK’s next adequacy decision.

- ***EDPB Recital* – Ensuring that scientific research is conducted in the public interest is not a new requirement, but a clarification that reflects the intention of the original GDPR**. ‘Public interest’ is a key characteristic of genuine scientific research - for example, in advancing academic knowledge in a given field. It is also an established term under UK GDPR, and the subject of ICO guidance.[19] As a test, it ensures that processing activity must have some public interest purpose or outcome beyond any benefits to the data controller. The European Data Protection Board issued a preliminary opinion that describes how public interest is a pre-existing assumption of reuse for scientific research - so much so that it was not made explicit in the original drafting; but now that the wording is being clarified, ostensibly clarified but in our view broadened, we think it's important this implicit assumption – that scientific research must be in the public interest - is made explicit in the law.

- **Commercial research typically has fewer safeguards than academic research** - GDPR was drafted on the assumption that ‘scientific research’ was being conducted academically and in the public interest. This means the related safeguards assumed a research process consistent with academic settings – for example, accountability of the researchers to an academic institution, and the presence of mechanisms like research ethics boards. As well as being important to ensure parity between public and private sector innovators, commercial R&D should be conducted ethically to minimise potential harms to the public. One option would be to require those reusing data under these provisions to seek approval from an independent research ethics committee that meets the REC review criteria standards set by UKRI.[20] The Bill only mandates a similar expectation for medical research, but it should be considered a baseline for any research to qualify as ‘scientific’.

- ***ICO Guidance -*** The ICO published an updated response to the DUA Bill, which maintains that where Parliament has added a public interest test for scientific research, the ICO is **content to issue guidance on what is meant by the ‘public interest’ in the context of scientific research.**[21] This suggests the ICO views the introduction of a public interest test as a feasible amendment to the Bill.

- ***Public Health Provision –*** The government argues that introducing a public interest test for scientific research will place undue burden on scientists to define the outcomes of their work in advance, and

[18] European Data Protection Board (2020) *Preliminary Opinion on Data Protection and Scientific Research.*

[19] Information Commissioner’s Office, *UK GDPR Guidance and Resources: The Research Provisions – Principles and grounds for processing*

[20] UKRI (2024) Research organisations and research ethics committees

[21] Information Commissioner’s Office (2025) Information Commissioner’s updated response to the Data (Use and Access) (DUA) Bill – House of Commons

suggests that this will stifle scientists and prevent important scientific research from happening. However, existing provisions stipulate that a public interest test must be carried out for public health research, and this has not prevented important public health research from happening. The public interest test has not stifled public health research, and similarly would not stifle scientific research more broadly.

3. Recognised legitimate interests

Overview

The Bill permits the Secretary of State to make regulations that would allow processing under new grounds they specify with no consideration by the controller of the data subject's interests.

To lawfully process personal data, controllers need to have a 'lawful basis' under GDPR. Several of these grounds are available, such as having the data subject's consent. Another of the most commonly used is 'legitimate interests', which allows a processor (e.g., a company) to claim that they have a fair interest in collecting and processing someone's data for a particular purpose – for example, monitoring traffic on their website or managing their cybersecurity.

Crucially, this claim about their interests is safeguarded by **requiring the controller to apply a 'balancing test' that takes into account whether the interests of the data subject outweigh the controller's legitimate interest**; this fundamental protection avoids abuse of this pathway through GDPR and is the subject of extensive ICO guidance.

The Bill introduces a new ground of 'recognised legitimate interests', which essentially counts as a lawful basis for processing if it meets any of the descriptions in the new Annex 1 to GDPR (Schedule 4 of the Bill) – for example, processing necessary for the purposes of responding to an emergency or detecting crime.

While the new ground shares its name with 'legitimate interests', **it does not require the *controller* to make any balancing test taking the data subject's interests into account** – it just needs to meet the ground in the list.

The Bill gives the Secretary of State powers to define additional recognised legitimate interests beyond those in Annex 1, with some requirements.

What the Bill says

- *Clause 70* adds a new lawful processing basis of 'recognised legitimate interests', which means that a controller can show lawful grounds for processing if it meets a ground in Annex 1.

- *Clause 70(4)* gives the Secretary of State the power to add new recognised legitimate interests to Annex 1, provided they meet some requirements:

    - that they consider it appropriate to make the regulations having regard to the interests and fundamental rights and freedoms of data subjects and where relevant, the fact that children may be less aware of the risks and consequences associated with their data rights.

    - that the processing the new ground would enable is necessary to safeguard an objective listed in Article 23(1)(c-j) of UK GDPR.

- *Article 23(1)(c-j) of UK GDPR* lists these objectives: public security; crime; judicial independence /proceedings; ethics breaches for regulated professions; regulatory delivery of other objectives; the protection of the data subject or the rights and freedoms of others; the enforcement of civil law claims – and crucially, a very general objective:

  - “other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation matters, public health and social security”

- *Schedule 4* adds a new Annex 1, which contains a list of recognised legitimate interests largely falling under the list in Article 23(1) above.

- *Clause 106* specifies how the Secretary of State must consult before issuing regulations, only obligating them to consult the Commissioner and “such other persons as they consider appropriate”.

Proposed Amendments

Clause 70 – Lawfulness of processing

Amendment 11 – Restricting regulation-making powers of Secretary of State, with regards to adding new recognised legitimate interests

Amendment text:

Clause 70

Delete clause 70.

Explanation: This removes the new processing ground of recognised legitimate interest. The process of establishing a lawful ground is a fundamental component of protecting people’s data; the requirement is designed to create some friction in forcing the controller to justify why they are collecting and processing. Bypassing the consideration of data subject interests at this stage should only occur in exceptional circumstances.