Reset.

Data Protection and Digital Information (No. 2) Bill

Written Evidence from Reset (May, 2023)

About Reset:

Reset (www.reset.tech) seeks to improve the way in which digital information markets are governed, regulated and ultimately how they serve the public. We do this through supporting new public policies across a variety of areas — including data privacy, competition, elections, only safety, security, taxation and education.

Executive Summary

The Data Protection and Digital Information Bill No 2 (the '**Bill**') makes significant changes to the UK's data protection regime. Reset is concerned that these changes will undermine data rights, leave a question-mark over the UK's adequacy decision from the European Commission ('**EC**'), and fail to take advantage of this moment of reform to improve the UK's regime by supporting academic research and empowering consumers.

Supporting **academic research** is one of the Bill's principal objectives. The Bill's new operative definition of academic research is extremely broad, covering *'any research that can reasonably be described as scientific'*. This will indeed make research processing easier for controllers who already have large amounts of personal data – such as social media companies. But it will **extend permissive exemptions to their commercial activities** as well as true 'research'. Meanwhile, there is nothing in the Bill to assist genuine academic researchers in obtaining the data they need. Controllers currently lack any incentive to share personal data – a major barrier to research, including that into platform harms – and the Bill does not address this.

A range of changes in the Bill will **undermine data rights and disempower individuals**. In particular, a new legal test for the exercise of data subject rights – like the right of access – could make them harder to enforce. New rules and time limits for complaints means data subjects face waiting 20 months or longer to resolve even basic breaches of their rights through the regulator - double the current time due to the need for a free-standing complaint to secure copies of the personal data in question. And vaguely defined 'recognised legitimate interests' does away with the important requirement that controllers consider the interests of data subjects in their activities. Alongside an undermining of the accountability regime, the changes will lead to **more hidden processing, more complaints and litigation from data subjects, and a lower level of confidence from consumers** in how their data is used. Undermining data rights could also **reduce the practical effectiveness and influence of the Age Appropriate Design Code**, a major regulatory success-story for the UK. The Code has now been adopted by countries such as Ireland and the Netherlands, as well as in California, and the UK should be doubling down on this world-leading initiative, rather than increasing vulnerabilities to it.[1]

The Bill introduces a lower standard for transfers of data out of the UK than from the EU. Divergence between the countries granted 'adequacy' by the UK and EU respectively will necessitate complex geofencing and monitoring of data coming from the EU to the UK. The extensive reliance on secondary legislation in the Bill also introduces uncertainty about how the UK's regime will develop. As well as placing burdens on businesses**, these will leave a question mark over the long-term future of the UK's adequacy decision from the EC**, which could be challenged by

[1] https://5rightsfoundation.com/Approaches-to-Childrens-Data-Protection---.pdf

campaigners before the European Court of Justice (as the *Privacy Shield* for transfers of data to the US was) disincentivising investment in the UK.

The Bill's **new definition of personal data** could have unpredictable consequences, increase instances of reidentification from anonymous data by hostile actors, and/or lead controllers to rely on spurious legal arguments in an attempt to take important types of processing outside the scope of the data protection regime. These impacts appear to be unintended but changes to the Bill in its most recent version have not addressed these risks.

This, the first opportunity to reshape the UK's data protection regime since Brexit, **misses important opportunities** where data rights could be enhanced, innovation facilitated, and the Government's stated objectives better met:

- The Bill **fails to create an incentive or requirement for controllers to share the data they hold with academic researchers**. A proposed amendment to the Online Safety Bill[2] shows how this can be done in a particular area of research, while still remaining privacy respecting without infringing on trade secrets.
- The Bill should implement Article 80(2) of the UK GDPR, **allowing representative bodies to bring complaints and claims about data protection breaches**. This would be a significant boost to consumer empowerment.
- The **right to data portability** in the UK GDPR has significant potential for business competition and innovation, and could help consumers realise the

[2] https://www.reset.tech/documents/data_access_ammendment_online_safety_bill.pdf

full benefits of decentralised digital technologies. The Bill should be used to **reform this right and make it effective** in relation to today's technologies.

The Secretary of State has described[3] the Bill as enabling academic research, friendly to consumers, and focussing protections on high-risk processing and large firms. Reset is concerned that in its current form the Bill achieves none of these stated objectives and significantly weakens data rights and privacy protections for UK users. It entrenches the power of large controllers without opening up access to data for research, at the expense of SMEs and academic research. (This is also in direct contradiction with the recently introduced Digital Markets, Competition and Consumer Bill which seeks to tackle anti-competitive behaviour). It undermines consumer empowerment and puts a heavy burden on individuals to enforce their rights. And it will create a system of dual compliance of little benefit and significant cost to any business – large or small – that handles EU citizens' data.

Our submission outlines in detail Reset's concerns, alongside suggestions for how the Bill may be amended to mitigate them..

3 https://www.express.co.uk/comment/expresscomment/1758848/data-protection-bill-brexit-news-nuisance-calls-businesses-comment

Table of Contents:

1. Impact on Data Rights

Summary: The Data Protection and Digital Information Bill (the 'Bill') introduces significant changes to the data protection regime that threaten to undermine data rights.

In the new 'recognised legitimate interests' legal ground for processing and permissive rules on further processing, the Bill creates extensive new grey areas in which controllers will be free to interpret the GDPR loosely and in the way most convenient to their processing. The net result will be more hidden processing, fewer data subject rights, and the need for more complaints and challenges from data subjects.

At the same time, the new 'vexatious or excessive' test for the exercise of data subject rights places new barriers in front of data subjects. Our analysis suggests the new rules and time limits for complaints means data subjects face waiting 20 months or longer to resolve even basic breaches of their data rights.

Even where such challenges are successful, it is rarely possible to completely 'undo' processing that has already taken place. Processing under this new more flexible regime could have a lasting impact on data subjects, even where they successfully challenge it.

'Recognised Legitimate Interests'[4]

No consideration of data subjects' interests

1. s.5 of the Bill creates a new lawful basis for processing in a new Article 6(1)(ea) UK GDPR – recognised legitimate interests (REIs). This lawful basis shares little with the existing 'legitimate interests' lawful basis[5], as it creates an automatic basis for

[4] Note that s.5 of the Bill gives examples of interests which may be legitimate interests – but *not* of 'recognised legitimate interests'. The addition of these non-exhaustive examples does not meaningfully alter the operation of the legitimate interests lawful basis.

[5] Although, like legitimate interests, it attracts the right to object to processing under Article 21 UK GDPR.

processing that is ‘necessary’ for any one of a set list of interests (at Annex 1 of the Bill), which may be amended by the Secretary of State.

2. Of most concern is that there is no requirement for controllers to consider whether or how data subjects’ interests against the processing might outweigh their own (which the wording of Article 6(1)(f) implicitly requires controllers to do when relying on legitimate interests under the current regime, and which is mandated by ICO guidance under the UK GDPR). Nor is there even a requirement for controllers to document why their processing is necessary for an RLI, making it difficult for data subjects to assess the lawfulness of the processing of their personal data.

3. The Government states in its consultation response that some controllers are *‘concerned about the time and effort required to complete and record their legitimate interest assessments’.* The Bill addresses this need for an assessment by simply doing away with a vital safeguard for data subjects in a wide range of processing contexts.

4. This is especially concerning as the RLIs can be used by any non-public authority controller, and some of the RLIs proposed in the Bill are broad and vague, including:

   i. ‘detecting, investigating or preventing crime’; and
   ii. ‘democratic engagement’.

Interaction with vague processing purposes

5. It is foundational to the GDPR regime that each act of processing has a purpose; for example, assessing whether there is a lawful basis for processing under Article 6 requires a consideration of the purpose of the processing. Data rights are best protected where controllers identify with specificity for which purposes they process which data. In practice however, controllers often list *all* of their purposes (vaguely defined, and often

relying at least in part on legitimate interests), and *all* of the data they process, with no indication of which data is processed for which purposes (see e.g., Google's privacy policy and related legal challenges[6]).

6. The (over-)use of and / or overreliance on RLIs is likely to exacerbate the problem of using data for collateral purposes without an appropriate legal basis, as the existence of predetermined RLI incentivises data controllers to attempt to fit their processing (or at least part of it) into one of the RLIs. There is a real risk that controllers would stretch the definition of one or more RLIs to cover at least some of their processing, giving themselves flexibility over a wide range of processing and personal data, without an explicit requirement to consider how that processing affects data subjects. Even under the existing GDPR regime, we already see some controllers (e.g., private facial recognition companies[7]) using the 'prevention of crime' as a justification for extensive and intrusive processing at significant scale, primarily for private commercial purposes.

Consider a 'gig economy' fast food delivery company that processes a wide range of data on its workers, including minute-by-minute location data. Location data processing may be primarily for performance management (e.g., setting and monitoring against target delivery times). In extremis, location data might be used by the controller to detect crime (e.g., fraud by workers via false statements about how long they have had to wait for an order to be ready for delivery).

There is a temptation for the controller to state in their privacy policy that location (and other) data is processed for both these purposes and on the basis of the controllers' legitimate interests, without particularising *which* processing is for the detection of

[6] https://policies.google.com/privacy?hl=en-GB and https://www.iccl.ie/digital-data/gdpr-complaint-against-googles-internal-data-free-for-all/

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

crime. It is easier to provide fewer details, and the prevention of crime sounds like a compelling justification for processing, making it harder to challenge the processing of location data.

Under the current regime, there is at least the (limited) protection that the controller must consider (and document) the balance of their interests and those of the platform workers. Under the new regime, the temptation for the controller to conflate their performance management and crime prevention purposes will be even greater:

7. The Bill could be improved by:

i. Preventing reliance on the lawful basis where data subjects' rights and interests override those of the controller (as is the case for the legitimate interests lawful basis – Article 6(1)(f) UK GDPR); and/or

ii. Requiring controllers to document and publish (e.g., in a privacy notice) an assessment of their reliance on an RLI – i.e. why their processing is necessary for the specific purpose, and clearly delineating which of their processing activities they consider fall within the RLI; and/or

iii. Removing the Secretary of State's discretion to change the list of RLIs.

Barriers to exercising data rights (substance)

Vexatious or excessive data subject requests

8. s.7 of the Bill inserts a new Article 12A into the UK GDPR which allows controllers to refuse the exercise of data subject rights in Articles 15 to 22 and 34 where the exercise is '*vexatious or excessive'*. These rights include the right of access, right to erasure, and right to object to processing.

9. 'Vexatious or excessive' replaces the current test in the GDPR under which requests can only be refused or charged for where they are *'manifestly unfounded'* or excessive. The intention of the change appears to be to afford controllers more discretion in refusing or charging for requests. For example:

i. New Article 12A(4) UK GDPR 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 not at all clear whether or how such factors militate in favour of or against a request. For example, in the data broking sector[8], there is little or no relationship between the data subject and the controller, such that the processing is hidden or 'invisible'[9]. Would this tend to indicate that a request under the GDPR is vexatious? Conversely, would an employment or work context, in which the controller and data subject have a close and complex relationship, militate in favour of or against a determination that a GDPR request was vexatious? The Bill itself is unclear, and the examples given in the Government's consultation response[10] both appear to describe situations which would be covered by the current, 'manifestly unfounded' test.

ii. New Article 12A(5) UK GDPR gives as examples of vexatious requests those that are 'an abuse of process' – wording mirroring concepts in civil litigation that sits uncomfortably in the context of the exercise of fundamental rights.

---

[8] See e.g https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2020/10/ico-takes-enforcement-action-against-experian-after-data-broking-investigation/

[9] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-%20regulation-gdpr/principles/lawfulness-fairness-and-transparency/

[10] https://www.gov.uk/government/consultations/data-a-new-direction/outcome/data-a-new-direction-government-response-to-consultation#annex-b-list-of-organisations-that-responded-to-the-consultation

10. The new test reflects language used in the Freedom of Information Act 2000 (FOIA). “Vexatious” in FOIA requests has been interpreted by courts to have a particular meaning, with the starting point of the reasoning being that considering a FOIA request needs an “objective standard” looking for a "reasonable foundation" of "value to the requester" (or the public)[11]. This suggests controllers may be able to ask data subjects for their reasons for exercising their data rights – something not permitted under the current regime. Such a process would cause delay and increase avenues for controllers to refuse requests or tie data subjects up in lengthy correspondence, frustrating their rights. It would be particularly concerning if controllers used the fact of data subjects’ awareness that a rights request might cause the controller discomfort to characterise it as ‘vexatious’. Indeed, it is often in such cases that the facilitation of data subject rights and the rebalancing of power away from the data controller is of greatest importance. A request that is inconvenient to a controller is no less valid.

11. Many data controllers – particularly those whose business models rely on processing large amounts of personal data – are reluctant to give effect to the exercise of data subject rights[12]. The new ‘vexatious or excessive’ test threatens to hollow out the rights under Articles 15 to 22 UK GDPR. This is particularly concerning for:

i. The right of access, which is foundational to all other data rights. If data subjects cannot find out how their data is being processed, they cannot ensure that the processing is lawful, exercise their wider rights or have any meaningful control over their information.

---

[11] https://ico.org.uk/for-organisations/guidance-index/freedom-of-information-and-environmental-information-regulations/dealing-with-vexatious-requests-section-14/what-does-vexatious-mean/

[12] See for example a report from Worker Info Exchange on challenges for gig economy workers exercising the right of access: https://www.workerinfoexchange.org/wie-report-managed-by-bots

ii. The right to object. This includes an absolute right to object to processing for direct marketing processes which should not be unduly diluted by greater freedom for data controllers to refuse it on vague grounds.

12. Whilst Article 12A(3) in theory places the burden of demonstrating a request is vexatious on the controller, in practice data controllers are in control of actioning a request, meaning that it will often be for data subjects to argue that their request is *not* vexatious. The Bill does not oblige controllers to give data subjects a reason for a refusal based on Article 12A(2); data subjects who do not even know why a request has been refused will find it very difficult to demonstrate – whether to the controller, the Information Commissioner, or a court, that their request is not vexatious or excessive.

13. Even where controllers opt to charge a fee rather than refuse a vexatious request outright, this could be a barrier to the exercise of data subject rights to the point of frustrating them entirely. The Bill does not mandate how controllers can levy such a fee, leaving space for delay (e.g., where controllers insist on payment by cheque or to a third country using intermediaries).

Reduced accountability requirements

14. The Bill makes a number of changes to the mechanisms provided for controller accountability in the GDPR which will make compliance with data subject rights more difficult. Most notably:

i. s.13 of the Bill removes the requirement for controllers based outside the UK to nominate a representative in the UK. This is likely to create additional barriers to the exercise of data subject rights, requiring international correspondence and – in combination with Article 12A – the payment of fees internationally.

ii. s.15 of the Bill restricts the requirement to keep any records of processing to controllers carrying out 'high risk' processing. Even in this case, controllers need only record the *categories* of recipients of personal data rather than the actual recipients[13]. It is not always possible to know in advance which processing is high risk. The Bill creates the situation that high risk processing becomes evident, only for there to be no records of how data subjects' personal data has been processed, creating a significant barrier to data subjects being able to exercise their rights or seek redress for unlawful processing.

15. We expect the impact of these changes to be:

i. A significant increase in the number of refused requests under Articles 15 to 22, directly undermining data rights.

ii. An increase in the number of 'satellite' complaints about the right of access, preliminary to substantive complaints about processing, before the Information Commission and the courts (with attendant costs).

iii. An increase in data subjects relying on pre-action disclosure under the Pre- action Protocol for Media and Communications Claims, where they are unable to establish how their data is being processed using Article 15 UK GDPR, in turn increasing costs for businesses.

[13] In the recent case *Österreichische Poste Case C-154/21* the ECJ held that when a data subject exercises his or her right of access, this includes information on the *specific* recipients of his or her personal data. The changes envisaged by the Bill would make compliance on this basis impossible for many data controllers. This is a notable change, despite ECJ cases no longer having precedential value in the UK.

16. The Bill could be improved by:

i. Retaining the existing test for the exercise of data subject rights – 'manifestly unfounded or excessive' – and removing the list of factors and examples at Article 12A(4) and (5); and/or

ii. Obliging controllers to give reasons to data subjects where requests are refused, or a fee is charged in reliance on Article 12A; and/or

iii. Extending the right to restrict processing under Article 18 UK GDPR to cover any period during which a dispute as to whether an exercise of the rights under Articles 16, 17 or 21 are 'vexatious or excessive'; and/or

iv. Requiring that any controller requiring a fee to be paid in reliance on new Article 12A GDPR nominates a sterling-denominated UK bank account for that purpose and provides for simple mechanisms for payments, such as debit card payment links.

<u>Barriers to exercising data rights (time limits)</u>

17. s.7 of the Bill introduces a new Article 12B UK GDPR, which gives data controllers greater flexibility in delaying responding to the exercise of data subject rights, including being able to ask for clarification merely by reason of processing a 'large amount of information concerning the data subject' (Article 12B(5)-(6)). Given many data controllers' business models, it is not at all clear why this alone should render a request unclear or in need of clarification. Indeed, this proposal creates a perverse incentive to gather more data.

18. §.39 and 40 of the Bill insert new sections (164A and B, and 165A and B) into the Data Protection Act 2018 (DPA). The combined effect is that data subjects *must* first

complain to the data controller before complaining to the Information Commission[14]. Whilst this reflects the Information Commissioner's Office approach under the current regime, the practical effect in combination with the likely increase in satellite complaints about the right of access, the impact could be that many complaints take *20 months* or longer to resolve. For the 10 months until the ICO determines that the user's access request is not vexatious or excessive, the user has no right to restrict or pause the processing complained of, heavily favouring the controller. The diagram below sets out how the Bill leads to this timeline.

19. The Bill could be improved by removing Article12B(6) (which gives processing a large amount of data as a specific reason for delaying a request) and by making the changes set out in para 16.

Lower standards for international transfers of personal data

20. s.21 and Schedule 5 of the Bill introduce a new UK-specific regime under which personal data may be transferred to third countries[15]. The main changes are:

i. The Secretary of State is empowered under new Article 45A to issue regulations ('approval regulations' herein) that permit the transfer of personal data from the UK to third-countries[16]. These approval regulations function in a similar way to adequacy decisions under the EU GDPR. They can be issued where the 'data protection test' under new Article 45B is met. This data protection test is analogous to the requirement in Article 45(1) EU GDPR that a country awarded an adequacy decision 'ensures an adequate level of protection' – which has been interpreted as meaning that the standard

[14] Article 165A(3) has the effect of creating a waiting period of 45 days from complaining to a controller to being able to complain to the Information Commission.
[15] We explore the new international transfers regime and its potential impact on the UK's data adequacy decision from the European Commission in a separate briefing paper in this set.
[16] A new Article 4(27) of the UK GDPR defines a third county as a country or territory outside the United Kingdom.

of data protection must be 'essentially equivalent[17]. The data protection test in Article 45B UK GDPR, however, is that the standard of data protection in the relevant third country is 'not materially lower' than that in the UK. It is not clear from the wording alone what is intended by this change from "essentially equivalent" to "not materially lower". Whilst the Government's consultation response states that the new regime will 'retain the same broad standard that a country needs to meet in order to be found adequate', it is difficult to see why the wording of the test would be changed, unless with the intention is to allow transfers to countries with lower standards of protection than currently qualify for adequacy under the EU GDPR.

ii. The data protection test in Article 45B differs from the adequacy test under the current GDPR regime in a number of respects, with the effect of giving the Secretary of State greater latitude in making approval regulations:

a. It does not require consideration of whether there is an independent and effective supervisory authority in the third country;

b. It replaces the need for 'administrative and judicial redress' with 'judicial or non-judicial redress' (a key issue in the Privacy Shield dispute).

c. it permits consideration of the 'constitution and traditions' of the third country, though it is not clear from the Bill – or the Government's consultation response – how such factors affect consideration of the data protection test.

iii. The Secretary of State may consider 'the desirability of facilitating transfers of personal data to and from the United Kingdom' (Article 45A(3)) in making regulations under Article 45A, which again appears designed to increase the range of countries in respect of which approval regulations may be made.

[17] Case C-362/14, *Schrems II*

iv. The 'data protection test' is used to assess the lawfulness of any standard data protection clauses promulgated by the Secretary of State under new Article 47A (effectively UK-issued standard contractual clauses).

21. The overall impact is that it is likely that controllers in the UK will have greater freedom to transfer personal data to a wider range of third countries than under the current regime (and by extension than controllers subject to the EU GDPR)[18]. Depending on how the UK's adequacy and standard clauses regime develops, this could significantly dilute the protection of UK data subjects' personal data.

22. Whilst the seemingly lower standard in the new data protection test is concerning, it reflects a high-priority policy objective for the Government.

23. The potential impact of these changes on the UK's own adequacy decision from the EU is discussed in section

Further processing for new purposes

24. s.6 clarifies when processing for purposes other than those for which personal data was collected ('new purposes') complies with the principle of purpose limitation. A new Article 8A creates notable new purposes that will be considered 'compatible' with the purpose for which data was collected (i.e. not in breach of the principle of purpose limitation[19]):

i. Ensuring or *demonstrating* that processing complies with Article 5(1) (Article 8A(3)(c)). It is not clear why controllers should be given greater freedom to carry out further

[18] Indeed this is consistent with stated UK government policy - https://www.gov.uk/government/news/uk-unveils-post-brexit-global-data-plans-to-boost-growth-increase-trade-and-improve-healthcare - and with the way these changes are described in the Government's consultation response.

[19] Where further processing is for a purpose deemed compatible with the original purpose, this does not *by itself* make the processing lawful: the further processing would still require a legal basis and must be fair and accurate (among other things). This is clarified by a new Article 5(3), inserted by s.6 of the Bill.

processing in an attempt to 'demonstrate' (perhaps spuriously or in vain) the lawfulness of their original processing.

ii. A specified list of purposes (Annex 2 of the Bill) including disclosures to *'any other person'* who makes a request which *'states that the other person needs the personal data for the purposes of carrying out processing'* for processing in the public interest (Article 8A3(d)). This appears to open up disclosures of a wide range of personal data to an unknown number and range of other controllers. The requirement that a request merely 'state' the relevant circumstances – rather than a requirement that those matters be true or demonstrable – also offers very weak protection for data subjects.

25. Article 8A(3)(e) also states that a new purpose will be compatible where it is 'necessary to safeguard an objective listed in Article 23' (public security, emergencies etc.). This contrasts with the current wording of Article 6(4) which makes new purposes compatible where they are:

"based on a Union or Member State law ***which constitutes a necessary and proportionate measure in a democratic society*** *to safeguard the objectives referred to in Article 23(1)"* (emphases added)

26. The removal of the emphasised words appears to remove an important safeguard. Alongside the list of recognised compatible secondary purposes introduced by Article 8A(3)(d), the effect is to effectively do away with the principle of purpose limitation in a range of security, regulation, and crime prevention contexts.

Consider for example a data collected for a relatively 'everyday' purpose – such as in the context of the running of a small business (the 'first controller') – which is requested from the first controller by another person (the 'second controller', which need not be a public authority) for the purposes of investigating crime. Under the current regime, the first controller would need to consider the factors listed in Article 6(4) GDPR to assess

whether further processing to make that disclosure was compatible with its original purpose. In many cases it will not be: there is no link between the original and secondary purposes, and there are potential negative consequences for the data subjects. This would make such further processing by the first controller unlawful, as it would breach the principle of purpose limitation.

Under the new regime, it will be enough for the second controller *merely to state* that it requires the data for processing that is (i) in the public interest, (ii) within Article 6(3) UK GDPR and s.8 DPA, and (iii) necessary to safeguard an objective listed in Article 23 UK GDPR. The first controller's processing for the disclosure will be deemed compatible by Article 8A(3)(d) and Annex 2 para 1 GDPR, removing a significant protection for data subjects against this kind of unexpected and potentially very consequential disclosure of their personal data.

27. The Bill could be improved by – at a minimum – requiring that the matters listed in Annex 2 para 1(b) be *true* rather than merely *stated* in a request. Alternatively, the processing for disclosures described in Annex 2 para 1 could be limited to disclosures to public authorities.

28. The new Article 8A(2)(c) replicates unclear language about the relevance of data engaging Articles 9 or 10, which have caused confusion under the current regime. The section reads:

"In making [a determination about whether a new purpose is compatible with an original purpose], a person must take into account, among

other things— […]

(c) the nature of the personal data, including whether it is a special category of personal data (see Article 9) or personal data related to criminal convictions and offences (see Article 10).”

29. This clause attempts to address when data may be used for further purposes without breaching the principle of purpose limitation, replicating the language of the existing GDPR in Article 6(4). That existing language is however unclear. It would be reasonable to assume that the greater the sensitivity of the data, the less likely further processing would be considered compatible with the initial purpose. However, it would not be unreasonable to read this clause as suggesting that processing engaging Articles 9 or 10 *may* be compatible with an original purpose. This tension has led to differing readings by academics and others, particularly in the context of using data for research. It is therefore unclear how 8A(2)(c) is to operate, as the clause does not clarify how to determine whether the greater the sensitivity the less / more likely the processing is to be compatible, nor whether, if the new purpose is compatible, the original exemption under Article 9 or 10 can be relied upon for the new purpose. It would be preferable for the clause to reflect the intended outcome. If it is designed to guard against using sensitive data for secondary purposes, the clause should use clearer language.

Expanded use of cookies

30. s.79 of the Bill amends the Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR). A new Regulation 6 PECR permits the deployment of cookies where this is *‘with a view to making improvements to the service’*, subject to a right to object to those cookies. This is a loose test, which would appear to cover a very wide range of use of cookies. It also appears to be subjective: if a controller or operator considers that the deployment will improve a service from their perspective (e.g. by increasing monetisation through increased surveillance and changes to choice architecture), then such a deployment would presumably be *‘with a view to making*

improvements to the service'[20]. It therefore places the burden of objecting to very extensive tracking- by-default online onto internet users, rather than placing the burden of collecting (free, informed, and unambiguous) consent onto controllers.

31. The use of cookies enables those placing cookies to share the data collected with third parties for the same purposes (Regulation 6(2A)(c); those third parties may be able to rely on the expanded freedoms for controllers provided for in the Bill (e.g. the broad definition of research, and/or RLIs).

32. This would have the effect of legitimising the means by which internet users can very quickly find their personal data has been transmitted through a vast network of third parties via the use of cookies (as is the case in the online gambling sector, for example[21]).

33. It may be true that current practices by which website operators purport to gather consent for the placement of cookies on users' browsers are unpopular with internet users. However, many operators are engaged in 'compliance theatre' rather than genuinely trying to comply with the law or protect users' interests. Indeed, the consent notices such operators use are being challenged for their attempts to work as compliance tools[22]. Those challenges are proving successful, because the intention behind the consent mechanisms is not to meet legal requirements but to frustrate users; the real problem with consent pop-ups is lack of compliance with the law rather than the law itself. The answer to operators creating deliberately frustrating and confusing means to gather invalid consent to cookies is not to legalise complex and pervasive architectures of surveillance online, but to fully enforce the laws designed to protect

[20] It is notable however that some major advertising bodies do not believe that the changes would permit the use of advertising cookies without consent. See e.g. https://www.iabuk.com/news-article/what-do-data-protection-changes-mean-digital-advertising

[21] https://cdn.sanity.io/files/btrsclf0/production/2018e1d767bd4146d49cc9d854d24b9cd5c984a7.pdf

[22] https://www.awo.agency/latest/the-tcf-decision-and-the-future-of-digital-advertising/

users data rights when they use the internet. The net effect of amending the law to facilitate the deployment of such cookies will be increased surveillance and reduced choices for consumers.

34. The bill could be improved by:

i. Retaining – and strengthening – the requirement that website operators obtain freely given, informed, and unambiguous consent to the placement of cookies for the purpose of service improvements; and/or

ii. Reducing or more narrowly defining the list of purposes in new Regulation 6(2A) PECR (e.g. requiring 'improvements' to be considered exclusively from the user's perspective).

35. s.81 of the Bill creates a definition of 'direct marketing' – previously undefined. This is a positive change and likely has a broader impact given the term is used elsewhere (e.g. in Article 21 UK GDPR). A further positive change is the extension of GDPR-level penalties to breaches of PECR (s.86 and Schedule 10 of the Bill).

36. Note that the Bill envisages regulations making provision for the recognition of technology for users to communicate automatic opt-out signals for cookies, which would, when developed (per the Government's consultation response), underpin an opt-out model for *all* cookies.

2. Missed opportunities

In the context of the first opportunity to reshape the UK's data protection regime since Brexit, there are a number of notable missed opportunities in the Data Protection and Digital Information Bill (the 'Bill') where data rights could have been enhanced, innovation facilitated, and the Government's stated objectives better met:

- The Bill fails to overcome one of the main barriers to data-driven research, the fact that those large controllers have no reason to share the data they hold with academic researchers.
- The Bill does not implement Article 80(2) in English law, which would have significantly improved standards of data protection by allowing representative bodies to bring complaints about breaches of the law;
- The Bill leaves the right to data portability unreformed and ineffective. This right not only has significant potential for business competition and innovation, but could help consumers realise the full benefits of decentralised digital technologies.

The Government should take this rare opportunity to make improvements to the UK's data protection regime that have long been advocated and would benefit researchers, individuals, and businesses.

<u>Failure to incentivise *sharing* of data for research</u>

1. The Bill's provisions on scientific research do not grapple with the principle current barrier to research processing in the GDPR: that it creates no incentive or obligation on the part of controllers to share data with third parties for scientific

research. Given the risks (even if they are only notional) of sharing personal data with third party researchers, controllers with large amounts of data useful to researchers (such as social media platforms) have little reason to do so currently.

This dynamic has been articulated in a report by the European Digital Media Observatory, which both Meta/Facebook and Twitter themselves supported[23].

2. The Bill in practice gives greater freedom to *existing* controllers of large amounts of personal data to use their own data (with a further extension of the definition of scientific research in the latest version), without actively facilitating access to that data by independent researchers or other innovators. This puts a key objective of the Bill – to drive scientific research[24] - at serious risk. We strongly urge the government to amend this fatal flaw in the legislation to account for SMEs as well as academic and civil society research.

3. The Bill could be improved by the inclusion of an incentive or obligation on certain specified types of data controller to make personal data available to independent researchers for public interest scientific research. Article 40 of the EU Digital Services Act (the 'DSA') provides an example of how this is being achieved elsewhere. The DSA obliges very large platforms to make data available to vetted researchers for academic research into systemic risks in the EU. The European Digital Media Observatory's draft code under Article 40 GDPR and accompanying report indicating how a system of researcher data access could be implemented in practice, including establishing an

23 https://edmoprod.wpengine.com/wp-content/uploads/2022/02/Report-of-the-European-Digital-Media-Observatorys-Working-Group-on-Platform-to-Researcher-Data-Access-2022.pdf

24 https://www.gov.uk/government/consultations/data-a-new-direction/outcome/data-a-new-direction-government-response-to-consultation

organisation dedicated to vetting researchers and reviewing and mediating their requests for access to specific datasets.

Improving privacy protection through representative actions

4. The aim of the GDPR is to ensure the "effective and complete" protection of data subjects[1]. Article 80 GDPR seeks to further that purpose by assisting data subjects to assert their rights.

5. Article 80(2) provides:

"Member States may provide that any body, organisation or association referred to in paragraph 1 of this Article, independently of a data subject's mandate, has the right to lodge, in that Member State, a complaint with the supervisory authority which is competent pursuant to Article 77 and to exercise the rights referred to in Articles 78 and 79 if it considers that the rights of a data subject under this Regulation have been infringed as a result of the processing."

6. The intention behind Article 80(2) is to allow appropriately constituted organisations to bring proceedings concerning infringements of the data protection regulations in the absence of a data subject. That is, to ensure that proceedings may be brought in response to an infringement rather than on the specific facts of an individual's case. As a result, data subjects are – in theory – afforded greater and more effective protection of their rights.

7. Article 80(2) seeks to address infringements of the rights of data subjects at a macro level. Actions under it could address systemic infringements that arise by design, rather than requiring an individual to evidence the breaches and the specific effects to them.

Flaws in the existing Article 80(1) procedure

8. At present, an affected individual (a data subject) is always required in order to bring a claim or complaint to a supervisory authority. Indeed, the operation of data protection legislation is parasitic on a data subject. Whether through direct action or under s187 Data Protection Act 2018 ('DPA') (Representation of data subjects without their authority), a data subject will have to be named and engaged. In practice, a data subject is not always identifiable nor willing to bring action to address even the most egregious conduct.

9. Article 80(2) would fill a gap that Article 80(1) / s.187 DPA is not intended to fill. The Bill is the ideal opportunity for the Government to fully implement Article 80(2) GDPR in national law and plug a significant gap in the protection of UK citizens' privacy.

10. Article 80(2) recognises that there are instances where a data subject cannot be easily identified, or where a data subject might find it hard to evidence that they have been directly affected by the unlawful processing. Indeed, Article 80(1) / s.187 DPA is dependent on data subjects being sufficiently motivated by an identified (and identifiable) infringement of the data protection regulations. In practice, that process is not dissimilar to a data subject bringing such claims in their own name. That data subject would also have to engage an appropriate non-profit organisation, who is ready, able and committed to bring such an action. This will require consideration of that non-profit's mandate, resources and capacity.

11. Furthermore, even a motivated data subject may be unwilling to take action due to the risks involved. For instance, it would be reasonable for that data subject to not want to become involved in a lengthy and costly legal process which may be disproportionate to the loss suffered or remedy available. This is particularly pressing where the infringement concerns systemic concerns rather than where an individual has suffered material or non-material damage as a result of the infringement.

What Article 80(2) could provide

12. Introducing Article 80(2) would help to obviate the difficulties and limitations associated with an Article 80(1) / s.187 DPA action, including the administrative and evidential difficulties that would currently be associated with signing individuals up to a representative action under Article 80(1).

13. Moreover, the relevant non-profit should not need to identify the data subjects affected under Article 80(2). Rather, Article 80(2) GDPR supports the "effective and complete" protection of the Regulation where the non-profit considers that the Regulation is being infringed.

14. The lack of redress for the illegality within the Advertising Technology (AdTech) industry is one good example of how non-profit action under Article 80(2) against actors in that industry could ensure "effective and complete" accountability for systemic infringements of the GDPR. Had Article 80(2) GDPR been introduced, then it is inevitable that an organisation could have brought proceedings against the issues inherent in AdTech, including cookie "pop-up" notices. Article 80(2) would allow the courts to engage with the systemic issues that AdTech presents.

Any increase in the level of complaints would likely be modest

15. Any fears of the implementation of Article 80(2) creating a "floodgates" scenario would be misplaced. Indeed, similar "floodgates" arguments were made in the Article 80(1) GDPR context[25] yet the predicted deluge of cases has not materialised. There are a number of practical barriers within s187 DPA to the introduction of such actions leading to a deluge of actions and claims:

[25] See for instance Bird & Bird, 'The "Tidal wave" of data protection-related class actions: Why we're not drowning just yet…' (November 2018) < https://www.twobirds.com/en/news/articles/2018/global/tidal-wave-of-data-protection-related-cases> which observes that *"prior to the GDPR's entry into force in May this year, much was being said about the "inevitable" deluge of class actions likely to flood the UK court system as a result."*

i. An organisation has to meet two stringent qualifying criteria under §187 (3 – 4) DPA. Firstly, s.187(3) requires the organisation's constitution or enactment to have certain features including that it must be a non-profit and have objectives that are in the public interest. Secondly, s.187(4) DPA requires the organisation to be "active in the field of protecting data subjects' rights and freedoms with regard to the protection of their personal data". These criteria apply in an Article 80(1) context and should also apply to any action under Article 80(2).

ii. Nonprofits are restricted by their own lack of resources, and their mandate. As such, they are only likely to consider claims or other action in limited circumstances. In particular, such organisations would only consider such claims where there is a particularly meritorious matter that would otherwise not be brought. This is a high internal barrier that will limit the use and abuse of the mechanism. As such, any prospect that non-profits would bring speculative or spurious claims is remote.

iii. Fears that a non-profit may "go rogue" and bring complaints or actions that a data subject would be dissatisfied with are similarly unfounded. Whichever mechanism is introduced would not enable the organisation to seek monetary redress for themselves or a data subject but rather to test the legality of practices.

iv. Properly constituted bodies will only bring such issues to the regulator or court where they have identified an infringement of the GDPR/DPA, which is within their mandate to consider, and where no other actor is bringing the action.

v. While a non-profit may be able to bring a compensation action, depending on if and *how* Article 80(2) is introduced, it will not receive that compensation itself. This adds a further layer of protection should the ability to claim compensation for data subjects be granted to non-profits.

vi. For any damages claim, Article 82 GDPR requires a person to show material or non-material damage in order to be eligible for compensation. Non-profit organisations

would not be able to show such damage, particularly where the damages regime is tied to individual data subjects. If the non-profit were able to show damages for individual data subjects, then they would be able to claim for damages in their own right under Article 82 which would obviate the need for an Article 80(2) process.

vii. Furthermore, the court system and regulatory oversight mechanisms are well versed in dealing with and filtering unmeritorious claims and actions. As such, this is a further barrier to such actions being misused.

viii. Finally, the costs risks of bringing an action make cases and regulatory actions unlikely unless the organisation is willing to take those costs risks. Such risks will have to be weighed against the merit of the case and the lack of action by others to address the issue.

Making the right to data portability work

16. Article 20 GDPR gives data subjects the right to receive certain personal data which they have provided to a data controller, without hindrance and in an accessible format, and transmit that data to another controller. This is known as the right to “data portability”.

17. The right to data portability is intended to provide a number of benefits to consumers, including the ability to have their data transferred from one data controller to another when switching, for example, between energy providers or banks. Consumers can also request their personal data from, for example, music and video streaming websites, including the data which users create when browsing or using such sites (for example, their search or viewing history). Finally, technology in theory permits users to aggregate and monetise their own data through data unions and data trusts; a number of British companies are leading the development of such technology.

18. As currently formulated, however, the right to data portability is likely to be only of limited assistance to consumers. That limited right has not been enhanced in the Bill, contrasted to provision in the EU's Digital Markets Act which seeks to augment and improve the right to portability.

The scope of Article 20

19. Article 20 GDPR provides (emphasis added):

1. The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where:

(a) the processing is based on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) or on a contract pursuant to point (b) of Article 6(1); and

(b) the processing is carried out by automated means.

2. In exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.

3. The exercise of the right referred to in paragraph 1 of this Article shall be without prejudice to Article 17. That right shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

4. The right referred to in paragraph 1 shall not adversely affect the rights and freedoms of others.

20. A wide range of data held by controllers would constitute *"personal data concerning"* a data subject. As an example, personal data of a streaming site user (like their playlists and search history) is likely to be held in a way that relates to the user in question, making it their personal data[26]. Such data is also likely to have been *"provided"* by the individual user to the streaming site platform. The scope of *"provided"* data is intended to include data which results from the observation of the user's activity.[27]

21. The relevant data will ordinarily be processed either on the basis of *"contract"* (i.e. the terms and conditions of use of the relevant streaming site) or *"consent"*, and for most sectors and services, will be carried out by *"automated means"*, thereby fulfilling the basic requirements of Article 20(1) GDPR.

Limitations on the right

22. First, the right does not allow for real-time and continued porting of data, limiting the ability of individuals to pool their data and maximise innovation using that data. While Article 20 does cover multiple data portability requests,[28] it is unlikely to *require* controllers to provide users with a continuous real-time flow of their personal data. Article 20 only entitles a streaming site user to receive their data in a *"structured, commonly used and machine-readable format"*. Beyond these minimum requirements, Article 20 does not impose specific conditions relating to how, or how often, the user's data should be provided (Guidelines, p.17).

---

[26] See e.g. *Nowak v Data Protection Commissioner* (Case C-434/16) [2018] 1 WLR 3505
[27] Article 29 Working Party Guidelines on the right to data portability ("**the Guidelines**"), pp.9-10
[28] Article 12(5) GDPR allows a data controller to charge a reasonable fee or to refuse to act on a request where this is "*manifestly unfounded or excessive*". However, the Guidelines state at p.12: "*There should be very few cases where the data controller would be able to justify a refusal to deliver the requested information, even regarding multiple data portability requests. For information society or similar online services that specialise in automated processing of personal data, it is very unlikely that the answering of multiple data portability requests should generally be considered to impose an excessive burden.*"

23. Controllers can argue they are complying with Article 20 by providing users with an Excel spreadsheet of the data for example, which would hinder (or render impossible) the utilisation of such data in real-time. Whilst guidelines from data protection authorities suggest that the use of an externally accessible API may be *"a practical way"* of accommodating data portability, crucially they do not state that the use of such an API is, or can be, *required*. Many platforms now offer a "download your data" tool to data subjects, which may be used to achieve / show compliance with the right to portability, whilst limiting the practical utility of portability for data subjects.

24. Article 12(3) GDPR allows a data controller up to one month to respond to a data portability request and may allow up to three months in respect of complex and/or numerous requests. The specification of a defined (and relatively lengthy) response period further militates against interpreting Article 20 as conferring a right to real-time data portability.

25. It may further be disproportionate for a data subject to insist that their data be provided to them in a very specific format. While no express proportionality requirement is contained in Article 20, a court, tribunal or regulator may well use a proportionality analysis in practice[29]. Where users are seeking to monetise their data, that fact is likely to be relevant to any such proportionality assessment, given that a key (albeit not exclusive) focus of the right to data portability as it is currently formulated is to enable consumers to switch suppliers and/or service providers.

26. Thus, Article 20 is in practice a limited right that does not allow for innovative real-time porting and reuse of data.

---

[29] See, by analogy, *Zaw Lin v Commissioner of Police for the Metropolis* [2015] EWHC 2484 (QB). Although *Zaw Lin* concerned a request for information made under the (now repealed) Data Protection Act 1998, it illustrates that the court will be concerned to ensure that even data requests which engage fundamental rights are proportionate.

27. Second, the right to data portability under Article 20 is conferred only on the individual users of streaming sites (i.e. the 'data subjects'), rather than on any third parties developing technology which enables real-time data porting.[30] Where a data subject mandates such third parties to act on their behalf, they will nevertheless be subject to the original controller's terms of service. If those terms preclude real-time data porting, third party developers would not be permitted to implement that technology on the relevant platform. This is likely to constitute a significant practical barrier to real-time porting by individual data subjects.

Recognition of limitations of the current regime

28. The current limitations on the right to data portability have recently been the subject of consideration by the European Commission[31]. The Commission recognised that *"as a result of its design to enable switching of service providers rather enabling data reuse in digital ecosystems the right has practical limitations"* (p.10). The strategy further notes that giving data subjects additional control over their personal data, including by facilitating real-time porting of such data, is likely to entail significant benefits for consumers, including by facilitating 'dynamic data portability' through decentralised digital technologies (pp.10-11 and p. 20). The Bill could and should seek to encourage such innovation, for the benefit of consumers and businesses.

Making the right to portability fit for purpose

29. The right to portability has serious limitations in that it does not allow consumers to port their data to third parties on a continuous, real-time basis. Addressing these

[30] Note that Article 20 is not covered within Article 80 GDPR, which allows for third party representation of data subjects in certain circumstances.
[31] European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, *"A European Strategy for Data"* COM (2020) 66
https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_en.pdf

shortcomings would make the right more useful and increase its use by consumers, promoting switching between services, competition, and innovation. It could also unlock models of consumer empowerment through decentralised technologies such as blockchain, and data trusts. The European Commission has indicated the right should be capable of expansion. The UK Government should take this opportunity to lead the way in updating the GDPR for the latest developments in digital technology.

3. Academic Research

Summary: Increasing the benefits from data-driven scientific research was one of the key objectives cited by the Government in bringing forward the Data Protection and Digital Information Bill (the 'Bill')[32]. However, the changes risk heavily favouring controllers who already hold a lot of personal data – like social media companies – extending opt-outs and exemptions to their commercial activity. At the same time the Bill does nothing to overcome one of the main barriers to data-driven research; the fact that those large controllers have no reason to share the data they hold with academic researchers. The Bill does not therefore meet this core objective of facilitating researcher access to data.

Excessively broad definition of research

1. s.2 of the Bill inserts a new definition of 'scientific research into Article 4 UK GDPR:

*"**any research that can reasonably be described** as scientific, whether publicly or privately funded, and whether carried out as a commercial or non-commercial activity. Such references include processing for the purposes of technological development or demonstration[…]"* (emphasis added).

2. Whilst Recital 159 UK GDPR stated that research should be interpreted *'in a broad manner'*, the Bill goes further, creating an unconstrained and subjective definition on which controllers can rely, widened further in the most recent iteration of the Bill. This approach creates two problems (i) less certainty for controllers and (ii) potential harms for individuals.

[32] *"We will simplify the legal requirements around research so scientists can work to their strengths."* - https://www.gov.uk/government/consultations/data-a-new-direction/outcome/data-a-new-direction-

3. The UK GDPR already gives controllers significant exemptions and freedoms where their processing is for scientific research, and these are expanded by the Bill. They include:

   i. The ability to collect unspecified consent (s.3 of the Bill and Article 4 UK GDPR)[33]
   ii. The ability to conduct further processing for new, scientific research, purposes (s. 6 of the Bill and new Article 8A UK GDPR).
   iii. Exemptions from providing transparency information about further processing for new, scientific research, purposes (s.9 of the Bill and Article 13 UK GDPR).
   iv. Longer retention periods (Article 5(1)(e) UK GDPR).
   v. Exemptions in some cases from the right to erasure (Article 17 UK GDPR).
   vi. Exemptions in some cases from the right to object (Article 21 UK GDPR).

4. The relaxation of GDPR provisions can be justified for genuinely scientific research with a degree of public benefit. This excessively broad definition, however, risks extending that relaxation to 'scientific research' processing by commercial controllers primarily for their own private benefit – e.g., for product development. It could lead to a significant expansion of processing for such commercial purposes whilst providing exemptions from fundamental data subject rights, making such practices effectively hidden from data subjects.

5. The Bill could be improved by a more considered definition of scientific research, for example requiring a consideration of its purpose, the field of enquiry, the type of controller carrying it out, and the methodological and ethical standards used. An example of how this has been attempted in the EU GDPR context is available from the European Digital Media Observatory, which has promulgated a draft code of conduct

[33] s,3(3) of the Bill inserts new paras (7) and (8) into the UK GDPR, which provide that consent meets the definition in the GDPR if it is for scientific research purposes, and those purposes are not fully identified when the consent is collected, subject to complying with ethical standards in research.

under Article 40 GDPR, intended to govern academic researcher access to data held by social media platforms[34].

6. s.22 of the Bill incorporates safeguards controllers are required to have in place when processing for scientific research purposes. This is largely uncontroversial, though the new Articles 84B(2) and (3) UK GDPR appear to be redundant, since processing *'which does not permit the identification of a living individual'* would not be processing of personal data and would therefore fall outside the scope of the UK GDPR.

7. Note that the Bill makes separate provision for research in the area of public health and approved medical research.

Failure to incentivise *sharing* of data for research

8. The Bill's provisions on scientific research do not grapple with the principle current barrier to research processing in the GDPR: that it creates no incentive or obligation on the part of controllers to share data with third parties for scientific research. Given the risks (even if they are only notional) of sharing personal data with third party researchers, controllers with large amounts of data useful to researchers (such as social media platforms) have little reason to do so currently. This dynamic has been articulated in a report by the European Digital Media Observatory[35], which both Meta/Facebook and Twitter themselves supported.

9. The Bill therefore gives greater freedom to *existing* controllers of large amounts of personal data to use their own data, without actively facilitating access to that data by

34 https://edmo.eu/wp-content/uploads/2022/02/Report-of-the-European-Digital-Media-Observatorys-Working-Group-on-Platform-to-Researcher-Data-Access-2022.pdf

35 Ibid.

independent researchers or other innovators. This puts a key objective of the Bill – to drive scientific research[36] - at serious risk.

Potential barrier to platform research through purpose limitation

10. New Article 8A (inserted by clause 6 of the Bill) generally *loosens* the provisions on purpose limitation, providing at Article 8A(3) for a range of situations in which new processing will be treated as compatible with the original purpose.

11. However, Article 8A(4), provides a carve-out where the personal data were originally collected in reliance on consent. The result is that, where data are collected in reliance on consent, any new *research* processing will *not* be consistent with purpose limitation (i.e. will be unlawful) unless further consent is collected. This holds even if collecting further consent would be very difficult or disproportionate.

12. The Bill (and existing UK GDPR provisions) allows controllers to obtain relatively broad consent to research at the point of data collection[37]. And many research datasets are collected using other lawful bases. However, Article 8A(4) would still leave a significant gap where it becomes unlawful to carry out research processing using certain datasets. This could be a particular issue in the context of research into platform harms to the extent that platforms place greater reliance on consent over time, which they may do in response to recent European Data Protection Board rulings on Meta's use of the 'contractual necessity' basis[38].

13. Importantly, this is a change from the current position. It will become *harder* to carry out research in some circumstances under the Bill's provisions than it is now.

14. The Bill could be improved by:

[36] https://www.gov.uk/government/consultations/data-a-new-direction/outcome/data-a-new-direction-
[37] See e.g. clause 3 of the Bill.
[38] Binding decisions 3, 4 and 5/2022 of the European Data Protection Board.

i. the inclusion of an incentive or obligation on certain specified types of data controller to make personal data available to independent researchers for public interest scientific research, as is contained in Article 40 of the EU Digital Services Act (the 'DSA'). That Article creates a regime for very large online platforms and search engines to be required to provide access to data to vetted researchers (meeting requirements in the DSA for academic research into systemic risks in the EU.

ii. Clarification that where data was originally collected in reliance on consent, further processing for research purposes may be compatible with the principle of purpose limitation in at least some circumstances, without the need to obtain further consent.

4. Age Appropriate Design Code

The Age Appropriate Design Code ('**AADC**') was published by the ICO[39] in September 2020 under s.123 of the Data Protection Act 2018 ('**DPA**'). It does not create freestanding legal obligations but acts as an aid to interpretation as to whether processing of the data of individuals under 18 is lawful under the UK GDPR.

The Data Protection and Digital Information Bill No 2 (the '**Bill**') would make a range of changes to the UK GDPR and DPA. Although it weakens data protection rights overall[40] the Bill does not have an immediate, direct impact on the AADC.

In the longer-term however, the Bill could have a material effect on the standard of protection offered by the AADC. The ICO must keep the AADC under review (s.126 DPA) and may amend or replace it (s.123(2) DPA). The Bill changes the process by which codes like the AADC are amended or replaced, in ways that may lead to more business-friendly provisions in future iterations of the AADC:

Secretary of State Approval: Under the current regime, amendments to the AADC are presented to the Secretary of State ('**SoS'**), who *must* lay them before Parliament (s.125 DPA). Clause 31 of the Bill inserts a new s.124D DPA which means that the SoS *first* approves any amendments, and *only if they are approved*, lays them before Parliament. This gives significantly more power to the SoS and could lead to a watering down of rights protection in any amended AADC depending on his/her political alignment or priorities.

[39] The Information Commissioner's Office. Under the Bill, this will be re-established as the Information Commission. We refer to the regulatory system both before and after any reform as the ICO.
[40] https://www.awo.agency/blog/the-data-reform-bill-uncertainty-and-missed-opportunities/

Panels: Clause 30 of the Bill inserts a new s.124B DPA which requires the appointment by the ICO of a panel of experts and (representatives of) those likely to be affected by an amended AADC. The panel will advise the commissioner on the amended AADC. Industry players have very significant resources available to them for public policy work; a panel considering amendments to the AADC could therefore become a vehicle through which protections are watered down.

Impact assessment: Clause 30 of the Bill inserts a new s.124C DPA requiring the ICO to conduct an impact assessment of any amended AADC. The ICO's draft Impact Assessment Framework heavily favours economic interests over data rights[41], meaning the new mandatory impact assessment under the Bill could lead to future iterations of the AADC being significantly more business friendly.

ICO Priorities: Clauses 27 and 28 of the Bill creates new constraints on how the ICO must carry out its functions, including amending the AADC. The ICO must have regard to the 'desirability of promoting innovation' (new s.120B DPA) and to other 'strategic priorities' designated by the SoS if approved by Parliament (new §120E-H DPA). The changes to how the ICO works are likely to make it more favourable to the interests of business in any amendments to the AADC.

In summary, whilst there will be no immediate change to the AADC, the Bill will change the way that the ICO carries out its work. Those changes mean that any future amendments to the AADC are likely to be more business friendly and place less of an emphasis on the importance of protecting children's data rights. Civil society will need to be alive to these concerns to the extent that the ICO looks to amend the AADC in future.

---

41 https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/ico-consultation-on-the-draft-impact-assessment-framework/.

5. International transfers and data adequacy

Summary: The Data Protection and Digital Information Bill (the 'Bill') introduces a lower standard for transfers of data out of the UK than from out of the EU. This presages divergence between the list of countries granted 'adequacy' by the UK and EU respectively, which will necessitate complex geofencing and monitoring of data coming from the EU to the UK. The extensive reliance on secondary legislation in the Bill also introduces uncertainty about how the UK's regime will develop.

As well as placing burdens on businesses, these changes may well leave a question mark over the long-term future of the EU's adequacy decision regarding the UK, disincentivising investment in the UK and causing difficulties for UK businesses.

Lower standards for international transfers of personal data

1. s.21 and Schedule 5 of the Bill introduce a new UK-specific regime under which personal data may be transferred to third countries[42]. The main changes are:

i. The Secretary of State is empowered under new Article 45A to issue regulations ('approval regulations') that permit the transfer of personal data from the UK internationally. These approval regulations function in a similar way to adequacy decisions under the EU GDPR. They can be issued where the 'data protection test' under new Article 45B is met. This data protection test is analogous to the requirement in Article 45(1) EU GDPR that a country awarded an adequacy decision 'ensures an adequate level of protection' – which has been interpreted as meaning that the standard of data protection must be 'essentially equivalent[43]. The data protection test in Article

[42] Note the most recent version of the Bill clarifies that any international transfer mechanisms that are lawful on the day the bill becomes law, will remain lawful.
[43] Case C-362/14, *Schrems II*

45B UK GDPR, however, is that the standard of data protection in the relevant third country is 'not materially lower' than that in the UK. It is not clear from the wording alone what is intended by this change from "essentially equivalent" to "not materially lower". Whilst the Government's consultation response states that the new regime will 'retain the same broad standard that a country needs to meet in order to be found adequate', it is difficult to see why the wording of the test would be changed unless with the intention is to allow transfers to countries with lower standards of protection than currently qualify for adequacy under the EU GDPR. **By doing this, the Bill would leave UK consumers and business constantly vulnerable to a future change in adequacy status. Such uncertainty would likely be a deterrent to foreign investment.**

ii. The data protection test in Article 45B differs from the adequacy test under the current GDPR regime in a number of respects, with the effect of giving the Secretary of State greater latitude in making approval regulations:

a. It does not require consideration of whether there is an independent and effective supervisory authority in the third country;

b. It replaces the need for 'administrative and judicial redress' with 'judicial or non-judicial redress' (a key issue in the Privacy Shield dispute).

c. It permits consideration of the 'constitution and traditions' of the third country, though it is not clear from the Bill – or the Government's consultation response – how such factors affect consideration of the data protection test.

iii. The Secretary of State may consider 'the desirability of facilitating transfers of personal data to and from the United Kingdom' (Article 45A(3)) in making regulations under

Article 45A, which again appears designed to increase the range of countries in respect of which approval regulations may be made.

2. The 'data protection test' is used to assess the lawfulness of any standard data protection clauses promulgated by the Secretary of State under new Article 47A (effectively UK-issued standard contractual clauses).

3. The overall impact is that it is likely that controllers in the UK will have greater freedom to transfer personal data to a wider range of third countries than under the current regime (and by extension than controllers subject to the EU GDPR)[44]. Depending on how the UK's adequacy and standard clauses regime develops, this could dilute the protection of UK data subjects' personal data.

EU's adequacy decision in respect of the UK

4. This change also implies the potential for personal data to be transferred from the EU to the UK (under the UK's adequacy decision from the European Commission), then onward from the UK to a third country not benefiting from an EU adequacy decision; this would undermine the EU GDPR.

5. The EU has sought to address a similar issue when granting its adequacy decision to Japan. As part of that decision, supplementary rules[45] provide for additional safeguards binding on Japanese companies importing data from the EU and enforceable by the Personal Information Protection Commission and Japanese courts. The supplementary rules include restrictions on onward transfers of data. In sum, if a Japanese business operator is transferring relevant EU personal data to a third country, informed consent of the EU data subjects is required unless the third party is in a

[44] Indeed this is consistent with stated UK government policy - https://www.gov.uk/government/news/uk-unveils-post-brexit-global-data-plans-to-boost-growth-increase-trade-and-improve-healthcare - and with the way these changes are described in the Government's consultation response.
[45] https://ec.europa.eu/info/sites/default/files/annex_i_supplementary_rules_en.pdf

country which is recognised to guarantee equivalent protections, or measures have been implemented (such as contract or other binding agreement) providing equivalent protections. Similar provisions apply to the adequacy decision for The Republic of Korea. That is, data transferred from the EU to Japan and Korea under the adequacy decisions must be both technically and legally 'geofenced' to protect it from onward international transfer.

6. It is possible that the UK's adequacy determination from the EU would be modified by similar supplementary rules (indeed this seems likely given the UK Government's stated intention to make regulations allowing transfers of personal data from the UK to a range of countries not benefiting from an EU adequacy decision). This would require geofencing of data transferred to the UK from the EU – a significant burden for UK controllers. Adherence to the supplementary rules would require ongoing monitoring by the EU, potentially leaving a question mark over the UK's adequacy decision, which could be challenged before the Court of Justice of the European Union (CJEU).This would not only be bad for data and consumer rights but would introduce unnecessary uncertainty for businesses, small and large, which might hinder future investment in UK products and services.

7. This issue could only be fully addressed by aligning the UK's own international transfers regime with adequacy decisions issued by the Commission, which is very unlikely. Short of this, an improvement would be to more tightly define the data protection test, to reduce the level of divergence between the lists of EU- adequate and UK-adequate jurisdictions.

Changes to law enforcement processing

8. The Bill makes a range of changes relevant to law enforcement and national security processing, including:

i. Clause 16, which removes the need for logging of the reasons for accessing certain data in law enforcement contexts.

ii. Clause 24, which expands the scope of the national security exemption in Part III of the Data Protection Act 2018 ('**DPA**').

iii. Clauses 25 and 26, which provide for greater scope for public bodies which are not intelligence agencies to carry out processing jointly with intelligence agencies within the scope of Part IV of the DPA.

9. Whilst these are not wholesale changes to the UK's regime for law enforcement processing, they have the effect of expanding the scope of law enforcement and intelligence processing and reducing safeguards for data rights. This is notable in the context of adequacy, since the *Schrems II* decision[46], which invalidated the 'Privacy Shield' route for data transfers from the EU to the US, turned heavily on issues of law enforcement and intelligence services processing. This could make the UK's intelligence services processing regime an obvious target for campaigners looking to challenge the UK's adequacy decision before the European Court of Justice in future.

Independence of the Information Commission

10. In granting an adequacy decision under Article 45 EU GDPR, the Commission must consider (inter alia) *"the existence and effective functioning of one or more **independent** supervisory authorities."* (emphasis added).

11. The Bill reduces the independence of the UK's supervisory authority – the ICO (to be renamed the Information Commission) – to a degree, which may undermine the UK's adequacy decision.

[46] European Court of Justice *Case C-311/18*

12. S.28 of the Bill introduces §120E-H into the DPA which, in sum, allow the Secretary of State to designate "strategic priorities" to which the Information Commissioner must 'have regard' (though these are subordinate to the Information Commissioner's principal objectives – s.120A). Whilst this is a significant change, s.120F(2) clarifies that the duty to have regard to the priorities does not apply when the Commissioner is carrying out specific investigations. It is doubtful therefore that this *alone* compromises the independence of the regulator to the extent that the test under Article 45 EU GDPR is no longer met.

Instability in the level of protection of personal data

13. The Bill makes extensive provision throughout for important provisions to be amended and varied by the Secretary of State through the introduction of statutory instruments according to various parliamentary procedures. These include adding interests in processing which may automatically qualify as a lawful basis without any need to balance them against data subjects' interests, among other matters which are fundamental to the protection of personal data.

14. Predicting the impact of this on the UK's adequacy determination requires a distinction between (i) the status and impact of the Bill itself on the day it becomes law, and (ii) the potential that it introduces for longer-term change to the UK's data protection regime.

Immediate impact

15. By leaving important matters of data protection subject to change through secondary legislation (i.e., without further primary legislation) and therefore full parliamentary scrutiny, it could be argued that the Bill creates a data protection regime that is too ill-defined and/or liable to change over time for the UK's adequacy decision to be meaningful. That is, the European Commission would not be able to assess whether

or not standards of data protection in the UK meet the relevant test in the EU GDPR for data adequacy.

16. It is unclear however, the extent to which the Commission is likely to inquire into the specifics of how secondary legislation is made in the UK, or whether it would be willing to effectively imply that the use of statutory instruments is arbitrary or not consistent with the rule of law. Article 45 EU GDPR also already provides for the protection of personal data in countries with adequacy to be monitored, which would allow the Commission to respond to any future fundamental reductions in data protection in the UK via statutory instrument. It is unlikely that the mere presence in the Bill of the ability to create secondary legislation would prevent the Commission from renewing the UK's adequacy determination, once it becomes law.

Longer-term impact

17. Over time, secondary legislation may lead to significant changes to the UK's data protection regime. There is likely to be anxious scrutiny of the way the UK's data protection regime is developing from the European Commission. Major changes could well prompt the Commission to reconsider whether the UK continues to meet the test in Article 45 GDPR.

18. Data adequacy is not only a political matter for the European Commission. It will face scrutiny before courts and data protection authorities. Individuals may bring cases before the CJEU (as has happened in relation to adequacy for the US) where they consider secondary legislation has changed the UK's regime to such an extent that an adequacy decision from the European Commission should no longer stand.

19. Thus while the role of secondary legislation in the Bill does not necessarily imperil the UK's adequacy on the day it becomes law, it leaves a real question mark over the long-term future of the UK's adequacy decision, depending on how that

secondary legislation is used to change the data protection regime. This in turn will undermine business confidence and investment.

20. To reduce this risk, the Government could limit the use of secondary legislation to less consequential aspects of the data protection regime.