DUA BILL AMENDMENTS: ORG STATEMENTS OF SUPPORT AND RATIONALE

Authors: Mariano delli Santi – mariano@openrightsgroup.org
James baker – james.baker@openrightsgroup.org
May 2025

In this document

Published by Open Rights, a non-profit company limited by Guarantee, registered in England and Wales no. 05581537. The Society of Authors, 24 Bedford Row, London, WC1R 4EH.

About Open Rights Group (ORG): Founded in 2005, Open Rights Group (ORG) is a UK-based digital campaigning organisation working to protect individuals' rights to privacy and free speech online. ORG has been following the UK government's proposed reforms to data protection since their inception.

ICO Complaints procedure for vulnerable individuals – statement of support for Siân Berry MP's amendment NC15

- The ICO acts upon the 0.00% of the (tens of thousand of) complaints it receives, effectively undermining UK residents' right to lodge a complaint under the DPA 2018.
- The Data Protection Act 2018 lacks a genuine avenue for judicial scrutiny or redress against the ICO decisions to drop complaints.
- People in a position of vulnerability have a greater need to protect their data, but are left powerless due to the ICO inaction.
- The House of Commons has an opportunity to address these concerns by supporting amendment NC15 tabled by Siân Berry MP.

The right to an effective remedy constitutes a core element of data protection: most individuals will not pursue cases before a court because of the lengthy, time-consuming and costly nature of judicial procedures. Also, act as a deterrence against data protection violations insofar victims can obtain meaningful redress: administrative remedies (such as enforcement notices or fines) are particularly useful because they focus on addressing malpractice and obtaining meaningful changes in how personal data is handled in practice.

However, the ICO has a long track record of refusing to act upon complaints: a recent Freedom of Information disclosure revealed that the ICO took "regulatory action" in just 1 (0.00%) case out of the 25,582 complaints lodged with them in 2024.[1]

Due to the Information Commissioner's Office poor performance of their duties, victims of egregious data protection violations have, perhaps, a greater chance of winning the lottery than finding meaningful redress by complaining to the ICO. **This includes people who may be in a position of vulnerability, such as victims of modern slavery, domestic abuse, gender-based violence, or victims of Violence Against Women and Girls (VAWG) who have a high need of privacy to protect themselves from abusers and stalkers.**

Likewise, the ICO has decided to drop ORG and several members of the public's complaints against Meta's reuse of personal data to train AI without carrying out any

1 See at: https://www.whatdotheyknow.com/request/proportion_of_complaints_you_rec/response/2895145/attach/3/IC%20353505%20C3D8%20Response%20Letter.pdf?cookie_passthrough=1

meaningful probe, despite substantiated evidence that Meta's practices do not comply with data protection law.[2] These include the fact that pictures of children on parent's Facebook profiles could just end up in their AI model as they are assuming consent, and yet the ICO has not even launched an investigation.[3] David Erdos (Co-Director at the Centre for Intellectual Property and Information Law at the University of Cambridge) noted that the ICO "has issued 0 fines & 0 enforcement notices against companies under UK GDPR for an entire year (going by its own published information)".[4]

Against this background, avenues to challenge ICO inaction are extremely limited: scrutiny of the Information Tribunal has been restricted to a purely procedural as opposed to substantive nature,[5] and it was narrowed even further by the Administrative Court decision which found that the ICO was not obliged to investigate each and every complaint.[6]

We recommend the House of Commons to address these concerns by supporting Siân Berry MP's amendment NC15, which would:

- Require the ICO to introduce an ad-hoc complaint procedure for people in a position of vulnerability, in order to ease their access to Justice;
- Give the right to individuals to appeal before the Information Tribunal ICO decisions to unjustly drop complaints.

This amendment would make it easier to people in a position of vulnerability to engage with and lodge a complaint to the Information Commission. Further, complainants would be provided with an effective avenue for redress before the Information Tribunal, which could review the substance of the Commissioner's response to their complaint. By allowing individuals to promote judicial scrutiny over decisions that have a fundamental impact into how Parliament laws are

2 See https://www.openrightsgroup.org/blog/the-ico-is-leaving-an-ai-enforcement-gap-in-the-uk/

3 See https://www.openrightsgroup.org/press-releases/org-complaint-to-ico-about-meta-privacy-policy-changes/

4 See David Erdos at: https://www.linkedin.com/posts/david-erdos-93827a11b_gdpr-dataprotection-databill-activity-7300455761669750784--k8o?utm_source=share&utm_medium=member_desktop&rcm=ACoAABI2y54BGnSWSOkQPBhcEtNW8rxDVlOqFNo

5 See Leighton v Information Commissioner (No. 2) (2020)103, Scranage v IC (2020), Killock and Veale, EW and Coghlan (2021)

6 See *Landmark Decision Handed Down on ICO's Responsibilities in Handling Subject Access Requests*, at: https://www.jdsupra.com/legalnews/landmark-decision-handed-down-on-ico-s-5683866/

enforced in practice, this amendment would also introduce a mechanism to promote accountability over how the new Commissioner uses their regulatory powers.

During the debate in the House of Lords, the government resisted these amendments by holding that the Information Tribunal would not be "competent" enough to scrutinise the substance of the ICO's determinations. However, Information Tribunal can already hear, and decide on the substance of, appeals against enforcement actions adopted by the ICO against data controllers—notably, enforcement notices and penalty notices. Indeed, both Experian[7] and Clearview AI[8] were able to challenge ICO notices on their merit before the Tribunal. In turn:

- If the Tribunal is considered "experienced" enough to judge on the merit of ICO decisions affecting data controllers, it is irrational to think they would be "inexperienced, informal or simply lacking appropriate procedure rules" to judge on the merits of decisions concerning data subjects.
- Well-resourced tech companies are allowed to challenge the ICO with a cheap and lean procedure before the Tribunal, while individuals are required to undergo a complex and expensive Judicial Review if they want to challenge an ICO decision on merit. This is unfair: data protection complaints should reduce the imbalance of power between individuals and controllers, but the status quo exacerbates this imbalance instead.

7 See Tribunal rules on Experian appeal against ICO action, at: https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2023/02/tribunal-rules-on-experian-appeal-against-ico-action/

8 See Information Commissioner seeks permission to appeal Clearview AI Inc ruling, at: https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2023/11/information-commissioner-seeks-permission-to-appeal-clearview-ai-inc-ruling/

International Data Transfers and rule of law requirements – statement of support for Alex Sobel MP's amendment 10

- International Data Transfers' (IDT) rules are an essential anti-circumvention measure that prevents organisations from transferring data to countries that lack strong data protection laws, where data can be accessed or misused in ways that would be illegal in the UK.
- Schedule 7 of the Data (Use and Access) Bill lowers' protection for IDTs, and risks undermining the foundations upon which the UK adequacy decision was built.
- Loosing the UK adequacy decision would cost UK businesses to 1-1.6£ billion costs in legal and compliance costs alone, and threaten the functioning of the EU-UK Trade and Cooperation Agreement and the Windsor Framework.
- The House of Commons has an opportunity to address these concerns by supporting Amendment 10, tabled by Alex Sobel MP.

Safeguards around International Data Transfers (IDT) are a fundamental component of data protection laws. Digital technologies and the Internet make it more likely that personal data may be stored or transferred outside of the UK: thus, ensuring that data protection rights "follow the data" is an essential safeguard against loopholes and data laundering.

In the UK GDPR, transfers may take place if the third country ensures an adequate level of protection. In essence, this framework is meant to ensure that individuals retain enforceable data rights and legal remedies regardless of the position their data is being stored.

Schedule 7 of the Data (Use and Access) Bill would lower protections for personal data transferred abroad, and give discretion to the Secretary of State to authorise IDTs regardless of the existence of enforceable rights and effective remedies. Further, and even in the absence of the authorisation of the Secretary of State, Schedule 7 would allow public and private organisations to transfer personal data to a third country without the need of proving the existence of enforceable rights and effective remedies.

The risk of these provisions are self-explanatory: if the UK becomes an avenue that allows organisations to bypass EU data protection law, the UK adequacy decision

will likely face invalidation by the Court of Justice of the EU or withdrawal from the European Commission. The UK was granted an adequacy decision by the European Commission in 2021, upon the basis that the UK data protection framework provided an equivalent level of protection to the EU GDPR. However, by lowering safety standards, the UK would be allowing organisations under its jurisdiction to transfer EU personal data to unsafe countries under the EU legal framework.

This risk is more than hypothetical: in the EU, civil society organisations have already denounced these same provisions, previously presented under the Data Protection and Digital Information Bill, and demanded that the European Commission "provide European citizens with assurance that it would repeal the adequacy decision if these proposals were to become law".[9] Likewise, the European Parliament expressed strong concerns about the compatibility of these proposals with UK adequacy and the EU-UK Trade and Cooperation Agreement, stressing that "the UK must ensure that its data transfers to non-EU countries are based on appropriate safeguards and that a level of data protection equivalent to that afforded by the European Union is guaranteed".[10]

By ignoring the threat of a judicial invalidation of the UK adequacy decision, the government risks exposing UK businesses to 1-1.6£ billion costs in legal and compliance costs alone, with an average of 10.000£ of legal costs for small and medium businesses.[11] Further, the invalidation of the UK adequacy decision would affect the functioning of the EU-UK Trade and Cooperation Agreement and the Windsor Framework, thus undermining the government efforts to further institutional and economic cooperation with the European Union.

Amendment 10 from Alex Sobel MP would amend Schedule 7 of the DUA Bill and ensure that a third country cannot be considered adequate or capable of providing appropriate safeguards.

---

9 See People Vs Big Tech, *Open Letter to the EU Commission regarding UK's data bill*, at: https://peoplevsbig.tech/open-letter-to-the-eu-commission-regarding-uks-data-bill/

10 See European Parliament, *OPINION OF THE COMMITTEE ON CIVIL LIBERTIES, JUSTICE AND HOME AFFAIRS (10.10.2023) for the Committee on Foreign Affairs and the Committee on International Trade on the implementation report on the EU-UK Trade and Cooperation Agreement*, at: https://www.europarl.europa.eu/doceo/document/A-9-2023-0331_EN.html#_section11

11 New Economic Foundation, *The cost of data inadequacy*, at: https://neweconomics.org/2020/11/the-cost-of-data-inadequacy

In particular, the amendment would unambiguously state that International Data Transfers (IDTs) cannot be authorised if:

- judicial protection of persons whose personal data is transferred to that third country is insufficient;
- effective administrative and judicial redress are not present;
- effective judicial review mechanisms do not exist; and
- there is no statutory right to effective legal remedy for data subjects.

Both the Conservative and Labour government have defended these provisions on the basis that they would not seek to use these powers to authorise IDTs that lower the protection afforded by the EU adequacy system. **If this is true, there is no valid reason the government should not approve this amendment and increase legal certainty over the UK international data transfers's regime.**

Further, and even assuming that the government would never use these powers to authorise data transfers to unsecure countries, Schedule 7 would still allow organisations to do so in the absence of a Secretary of State's authorisation. Amendment 10 would also address this concern as well, and prohibit public or private organisations from transferring UK residents' personal data to third-countries at the expenses, and to the detriment, of their rights.

SCHEDULE 7 IN DETAIL

Schedule 7 of the Data (Use and Access) Bill would replace Chapter 5 of the UK GDPR.

In particular, new Article 45A would empower the Secretary of State to make regulations approving transfers of personal data to third countries or international organisations. This regime would replace adequacy regulations under the UK GDPR, and in particular it would:

- **Give discretion to the Secretary of State to authorise transfers for reasons other than the level of protection for personal data.** According to New Article 45B, in determining whether the data protection test is met "the Secretary of State may have regard to any matter which the Secretary of State considers relevant, including the desirability of facilitating transfers of personal data to

and from the United Kingdom". This change must be seen in light of the intention to "boost trade" by "reducing barriers to data flows", including the possibility "to make adequacy regulations for groups of countries, regions and multilateral frameworks".[12]

- **Eliminate the requirement to consider "public security, defence, national security and criminal law and the access of public authorities to personal data", the existence of an independent supervisory authority and of effective judicial redress.** The CJEU has already invalidated two US adequacy decisions in the Schrems I and Schrems II judgements on the basis that these same requirements were missing; thus, the authorisation of IDTs to a country that lacks them would guarantee the revocation of the UK adequacy decision. However, new Article 45B only requires "respect for the rule of law and for human rights in the country or by the organisation", "the existence, and powers, of an authority responsible for enforcing the protection" and "arrangements for judicial or non-judicial redress" are considered in the data protection test, thus heightening the risk of an authorisation by the Secretray of State that would invalidate the UK adequacy decision.
- **Notably, even the Information Commissioner's Officer has agreed that the language of the law leaves ambiguity as to weather the Secretary of State's power to authorise data transfers having "regard to any matter they consider relevant" could override the requirement for the data protection test to be met,** and stated that "It would be helpful to clarify that the matters the Secretary of State may consider do not outweigh or take precedence over the need to meet the data protection test".[13] While this statement was related to the Data Protection and Digital Information Bill, the Labour government's decision to copy and paste the same provisions in the Data (Use and Access) Bill leaves this problem unaddressed.

Finally, Schedule 7 would amend Article 46 so that a transfer is considered to be subject to appropriate safeguards if an organisation acted "reasonably and proportionately", or if the Secretary of State specified standard data protection clauses under new Article 47A which "the Secretary of State considers are capable of securing that the data protection test".

12 Consultation outcome, Data: a new direction – government response to consultation: https://www.gov.uk/government/consultations/data-a-new-direction/outcome/data-a-new-direction-government-response-to-consultation

13 See *Information Commissioner's Response to the Data Protection and Digital Information (No 2) Bill (DPDI No 2 Bill)*, at: https://ico.org.uk/media/about-the-ico/consultation-responses/4025316/response-to-dpdi-bill-20230530.pdf

This would allow public and private organisations to consider an international data transfer subject to appropriate safeguards even in the absence of enforceable rights and effective remedies. According to Article 46 of the UK GDPR, appropriate safeguards must provide "enforceable data subject rights and effective legal remedies for data subjects". The enforceable nature of contractual clauses was identified as an essential element to ensure "appropriate safeguards" in the Schrems II judgement. However, the criteria introduced in Article 46 as amended by Schedule 7 does not consider the actual existence of enforceable rights and legal remedies, but only the due diligence of the organisation operating the transfer or the opinion of the Secretary.

The right to non-digital ID – Statement of support for Steff Aquarone MP's amendment NC7

Digital-only systems risk deepening exclusion. As increasing numbers of services move online, those without reliable internet access, digital skills, or ID documentation are being locked out. According to *Lloyds Bank's 2024 Consumer Digital Index*[14], around 23% of UK adults fall into the very lower digital kills category and 1.6 million people are still offline. For these individuals, digital-only verification systems—especially those involving apps or biometric scanning—can be insurmountable barriers to accessing services, entitlements, or employment. Amendment NC7 ensures that where non-digital alternatives are reasonably practicable, they must be offered, protecting inclusion and fairness.

Vulnerable groups are disproportionately affected. Research from *Age UK* and the *Digital Poverty Alliance*[15] has shown that older people, disabled individuals, recent migrants, and people experiencing homelessness are far more likely to be excluded by digital identity systems. The flawed E-visa rollout and the Home Office's switch to digital-only immigration status left thousands of people struggling to prove their right to work, rent, or access healthcare due to system failures or lack of digital

14 See Lloyds Bank's 2024 Consumer Digital Index report https://www.lloydsbank.com/assets/media/pdfs/banking_with_us/whats-happening/lb-consumer-digital-index-2024-report.pdf

15 https://digitalpovertyalliance.org/wp-content/uploads/2023/09/Deloitte-Digital-Poverty_FinalReport_29092023.pdf

access[16]. Offering non-digital options is a simple way to safeguard the rights and dignity of people in vulnerable situations.

Choice and trust strengthen, not weaken, security. Providing non-digital verification alternatives not only supports inclusion but also improves trust in the system. Some users are uncomfortable sharing sensitive personal data with private tech platforms or through opaque digital ID systems. Research from the Department of Science, Innovation and Technology - *Public dialogue on trust in digital identity services: a findings report attitudes to digital identity*[17] found that people thought paper alternatives should be available to digital ID systems. By mandating that alternatives be available where practicable, NC7 ensures the public can participate on terms that respect their privacy, reduce coercion, and promote confidence in both digital and non-digital processes.

16 See Computer Weekly 'UK eVisa system problems persist despite repeated warnings ' https://www.computerweekly.com/news/366618163/UK-eVisa-system-problems-persist-despite-repeated-warnings

17 https://www.gov.uk/government/publications/public-dialogue-on-trust-in-digital-identity-services/public-dialogue-on-trust-in-digital-identity-services-a-findings-report#benefits-and-concerns