DUA BILL: Evidence for the House of Commons Committee Stage

Author: Mariano delli Santi on behalf of Open Rights Group

February 2025

1. AMEND ARTICLE 6 OF THE UK GDPR TO PREVENT TECH COMPANIES FROM USING PERSONAL DATA WITHOUT CONSENT TO TRAIN COMMERCIAL AI MODELS 2
1. STRENGTHEN THE ICO STATUTORY OBJECTIVE 3
2. CURB THE ICO OVERRELIANCE ON NON-BINDING REPRIMANDS 5
3. STRENGTHEN THE INDEPENDENCE OF THE ICO 6
4. PROVIDE AN EFFECTIVE AVENUE FOR REDRESS FOR VICTIMS WHOSE COMPLAINTS ARE UNJUSTLY DROPPED BY THE ICO 8
5. DO NOT REDUCE ACCOUNTABILITY OVER DATA USES FOR LAW ENFORCEMENT AND PUBLIC SECURITY PURPOSES 12
6. DO NOT ALLOW THE GOVERNMENT TO OVERRIDE KEY ASPECTS OF DATA PROTECTION LAW WITH STATUTORY INSTRUMENTS 13
7. PROTECT GROW BY ADDRESSING THE THREATS TO THE UK ADEQUACY STATUS 15

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. (CC BY-SA 4.0).

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.

1. AMEND ARTICLE 6 OF THE UK GDPR TO PREVENT TECH COMPANIES FROM USING PERSONAL DATA WITHOUT CONSENT TO TRAIN COMMERCIAL AI MODELS

1. Several AI companies are bypassing requirements to seek individuals' consent to use their data for training commercial AI models by inappropriately relying on the legitimate interest legal basis.

2. A purely commercial legitimate interest does not reach the threshold to justify high-risk data processing activities such as those carried out by AI model developers. Under Article 6(1)f of the UK GDPR, a legitimate interest needs to reach a certain threshold, measured against the impact of data processing on an individuals' fundamental rights and freedoms, in order to be relied upon.

3. The Information Commissioner's Office has shown a tolerant attitude toward AI companies' data grabs and has left UK residents' data unprotected, making an unwelcome contrast with the assertiveness shown by European Data Protection Authorities (DPAs). In the EU, Meta was forced to suspend its plans to train AI on users' data.[1] The social media platform X had to sign an undertaking to suspend the use of EU personal for its AI model to avoid legal action.[2] Against this background, the Information Commissioner's Office has not only failed to protect UK residents from the same personal data abuses, but has boasted those as an example of how the ICO promotes economic growth in the UK.[3]

4. The argument that a consent-less use of personal data to train AI would be a stimulus to economic growth is extraordinary and ought to be rejected. As emerged from the debate around AI and copyright, promoting non-consensual uses of copyrighted material transfers wealth away from artists and creators toward large tech monopolies. **The same principle applies to personal data. Allowing the non-consensual exploitation of our personal information will grow the purses of tech companies without putting a single pound in our pockets.**

5. Responsible AI should ask for consent. We urge the House of Commons to table and approve an amendment that would clarify the meaning of Article 6(1)f, and clarify

[1]Tech Crunch, *Meta pauses plans to train AI using European users' data, bowing to regulatory pressure*, at: https://techcrunch.com/2024/06/14/meta-pauses-plans-to-train-ai-using-european-users-data-bowing-to-regulatory-pressure/

[2]Reuters, *Ireland's data regulator ends court proceedings against X*, at: https://www.reuters.com/technology/irelands-data-regulator-ends-court-proceedings-against-x-2024-09-04/

[3]See ICO response to government on economic growth, at: https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2025/01/ico-response-to-government-on-economic-growth/

that legitimate interest cannot be relied upon as a legal basis for the development of commercial AI models. This would ensure that AI companies have to seek consent when repurposing people's personal data for the training of commercial AI models. This would still allow the use of legitimate interest for open source and non-commercial AI development and research, provided that the rights and freedoms of individuals do not override such interest.

6. Proposed text for amendment

Amend the UK GDPR as follow:

After Article 6(2), insert:

(3) Point (f) of the first subparagraph shall not be relied upon to processing carried out for the purposes of developing Artificial Intelligence models whose components, including datasets, code, and model parameters, are not released free of charge and made freely available to use, study, modify, and share.

1. STRENGTHEN THE ICO STATUTORY OBJECTIVE

7. Clause 90 (Duties of the Commissioner in carrying out functions) of the DUA Bill introduces competing and ambivalent objectives that the new Information Commission would have to pursue, such as the desirability of promoting innovation, competition, national and public security, or to prevent crimes.

8. Data protection enforcement is important to ensure that innovation results in product and services that benefit individuals and society; to ensure that important public programmes retain the public trust they need to operate; and to ensure that companies compete fairly and are regarded for improving safety standards.

9. However, Clause 90 builds on the assumption that objectives such as innovation, economic growth and public security would be competing interests, and thus needs balancing against, data protection. By requiring the new Information Commission to adopt a more condoning and lenient approach on data protection breaches, Clause 90 would undermine the same policies it aims to promote:

- Innovation without any other connotation means merely new things, lacking any indication on whether these are desirable, able to solve existing problems, and benefit society as a whole. Only by ensuring strong data protection standards and human rights protection, we can ensure that the development and adoption of technologies translates into ethical, transparent outcomes that bring benefits for society and the individuals concerned.
- Policing and public security policies need public trust in order to be supported and accepted by the British public. Without effective supervision and

enforcement of data protection standards, important public security programmes only risk exposing already marginalised and over-policed communities to disproportionate targeting and discrimination. As ORG research has shown, poor data protection practices can lead to children being left behind and loosing out on life's opportunities due to unsubstantiated Prevent referrals lingering in a child's record for decades.[4]

- Economic growth depends on fair competition and fair commercial practices. As stated by the Government's Statutory Guidance on the growth duty, "T*he Growth Duty does not legitimise non-compliance with other duties or objectives, and its purpose is not to achieve or pursue economic growth at the expense of necessary protections. Non-compliant activity or behaviour [...] also harms the interests of legitimate businesses that are working to comply with regulatory requirements, disrupting competition and acting as a disincentive to invest in compliance"*[5]. The Guidance also identifies "Consistency – application of rules and policies are adopted and/or maintained with the minimum distortion to competition" and "Changing rules or other regulatory levers to help to level a playing field where justified competition should be occurring"[6] as indicators for regulators to ensure they are delivering competition benefits.

10. The Information Commissioner's Office has to close the enforcement gap The Information Commissioner's Office (ICO) did not serve a single GDPR enforcement notice in 2021-2022, secured no criminal convictions and issued only four GDPR fines totalling just £633k,[7] despite the fact that it received over 40,000 data subject complaints.[8] Fast forwarding to the present days, ORG's *ICO Alternative Annual Report* shows that the ICO issued just one fine and two enforcement notices against public sector bodies and "Only eight UK GDPR-related enforcement actions were taken against private sector organisations".[9] At the time this briefing is being written, 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)".[10]

---

[4]https://www.openrightsgroup.org/publications/prevent-and-the-pre-crime-state-how-unaccountable-data-sharing-is-harming-a-generation/

[5] https://www.gov.uk/government/publications/growth-duty PDF p.7

[6] Ibid, p.16

[7]See David Erdos, University of Cambridge, T*owards Effective Supervisory Oversight? Analysing UK Regulatory Enforcement of Data Protection and Electronic Privacy Rights and the Government's Statutory Reform Plans*, at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4284602

[8]See Information Commissioner, *Annual Report and Financial Statements 2021-22*, pp. 42, at: https://ico.org.uk/media/about-the-ico/documents/4021039/ico-annual-report-2021-22.pdf

[9]"ICO Alternative Annual Report 2023-4" (2024), Ohrvik-Scott, J; Killock, J; delli Santi, M. Open Rights Group: London. p. 9-15 https://www.openrightsgroup.org/publications/ico-alternative-annual-report-2023-24

[10]See David Erdos at: https://www.linkedin.com/posts/david-erdos-93827a11b_gdpr-dataprotection-databill-activity-7300455761669750784--

11. We recommend the House of Commons to retable Amendment HoL122 (Lord Clement-Jones). This would amend Clause 90 by clearly stating in legislation that the ICO have a duty of investigating infringements and ensuring the diligent application of data protection rules. If so amended, Clause 90 the DUA Bill would promote clarity and consistency in the ICO regulatory function: as pointed out by the Institute for Government, "Clarity of roles and responsibilities is the most important factor for effectiveness" of arms-length bodies,[11] such as the ICO.

2. CURB THE ICO OVERRELIANCE ON NON-BINDING REPRIMANDS

12. The ICO issued "28 reprimands to the public sector over the last financial year".[12] Reprimands are written statements where the ICO expresses regret over an organisation's failure to comply with data protection law, but they do not provide any incentive for change: a reprimand lacks legal force, and organisations face no further consequences from it. **Despite the fact that reprimands clearly lack deterrence, the ICO relies on reprimands extensively and against serious violations of data protection laws**, such as:[13]

- Police, prosecutors or the NHS exposed personal address details of victims of abuse, or witnesses to crime, to their abusers or those they were accusing, creating immediate personal, physical risks. In one example, the person affected had to move house.[14] In another, medical patients of the University Hospital of Derby and Burton NHS Trust (UHDB) did not receive medical treatment for up to two years.[15]
- Two police authorities, West Mercia Police and Warwickshire Police, lost the detailed records of investigations they had made, which could have impacted prosecutions or caused potential miscarriages of justice.[16]

---

k8o?utm_source=share&utm_medium=member_desktop&rcm=ACoAABI2y54BGnSWSOkQPBhcEtNW8rxDVlOqFNo

[11] See Institute for Government, *Read before burning*, p. 33, at: https://www.instituteforgovernment.org.uk/publication/read-burning-arms-length-bodies

[12] See figures in Open Rights Group, *ICO Alternative Annual Report 2022-23*, p.9 https://www.openrightsgroup.org/publications/ico-alternative-annual-report-2023-24/

[13] For full details of public sector reprimands issued after serious data protection failures, see *ICO Alternative Annual Report*, Appendix II p. 33-38.

[14] See https://ico.org.uk/media/action-weve-taken/reprimands/4025394/tvp-reprimand-20230530.pdf

[15] See https://ico.org.uk/action-weve-taken/enforcement/university-hospital-of-derby-and-burton-nhs-trust-uhdb/

[16] See https://ico.org.uk/action-weve-taken/enforcement/chief-constable-west-mercia-police-and-chief-constable-warwickshire-police/

- Two police authorities, Sussex Police and Surrey Police, recorded the conversations of hundreds of thousands of individuals without their consent.[17]
- Persistent failures by two police authorities and three local authorities to respond to Subject Access Requests in a timely fashion over periods of up to five years.[18]

13. Evidence proves that over-reliance on reprimands lacks deterrence for law-breaker. For instance, The Home Office was issued three consecutive reprimands in 2022 for a number of data protection breaches,[19] recording and publishing conversations with Windrush victims without consent,[20] and a systemic failure to answer to SARs within statutory limits, with over 22,000 requests handled late.[21] Against this background, the ICO issued yet another reprimand to the Home Office in 2024.[22] **The Home Office persistence in non-complying with data protection law is a good example of how reprimands, if not supported by the threat of substantive enforcement action, fails to provide a deterrence and thus gets ignored by the public sector.**

14. We recommend the House of Commons to retable amendment HoL123 (Lord Clement-Jones). This would impose a limit on the number of reprimands the ICO can issue to a given organisation without adopting any substantive regulatory action, such an enforcement notice and a fine. This would ensure the ICO does not evade its regulatory responsibilities by adopting enforcement actions that lack deterrence or the force of law.

3. STRENGTHEN THE INDEPENDENCE OF THE ICO

15. The Data Use and Access Bill would provide powers for the Secretary of State to interfere with the objective and impartial functioning of the new Information Commission, such as by discretionally appointing non-executive members of the newly-formed Information Commission (Schedule 14 – The Information Commission), or by introducing a requirement for the new Information Commission to consult the Secretary of State before laying a Code of Practice before Parliament for consideration (Clause 91 – Codes of practice for processing personal data, and Clause 92 – Codes of practice: panel and impact assessment).

---

[17] See https://ico.org.uk/action-weve-taken/enforcement/sussex-police/

[18] ICO Alternative Annual Report, p. 14

[19] https://ico.org.uk/action-weve-taken/enforcement/secretary-of-state-for-the-home-department/

[20] See: https://ico.org.uk/action-weve-taken/enforcement/secretary-of-state-for-the-home-department-home-office/

[21] See: https://ico.org.uk/action-weve-taken/enforcement/secretary-of-state-for-the-home-department-home-office-1/

[22] See: https://ico.org.uk/action-weve-taken/enforcement/home-office/

16. The guarantee of the independence of the ICO is intended to ensure the effectiveness and reliability of their regulatory function, and that the monitoring and enforcement of data protection laws are carried out objectively and free from partisan or extra-legal considerations. The recent change of **the of the Chair of the Competition and Markets Authority has focused concerns around independence of UK regulators**.[23]

17. Political pressure against the ICO has visibly increased over the years: in 2021, the Government framed the appointment of the new Information Commissioner as the first step in implementing their proposed reforms of the GDPR.[24] In turn, a cross-party group of Members of Parliament accused the Government to be seeking "an Information Commissioner whose policy views match its own, rather than a regulator that will seek to enforce the law as Parliament has written it".[25]

18. Correlation does not prove causation, but the Commissioner appointed as a result of that proceeding has expressed views on the DPDI Bill that, indeed, match those of the Government, despite widespread criticism coming from other arms-length bodies such as the National Data Guardian, the Biometrics and Surveillance Camera Commissioner, the Scottish Biometrics and Surveillance Camera Commissioner, and the Equality and Human Rights Commission.[26]

19. Correspondence revealed by a Freedom of Information request demonstrates that, after the DPDI Bill was dropped, the Information Commissioner expressed regrets over Parliament's decision and directed ICO staff to use its office discretionary powers to implement as much of the DPDI Bill as possible regardless of Parliament's will to drop that Bill.[27] Finally, the Information Commissioner has, once again, aligned his opinion to the government of the day and welcomed and fully supports the new DUA Bill,

---

[23]Sky News, *Chair of UK's competition regulator removed by government*, at: https://news.sky.com/story/chair-of-uks-competition-regulator-removed-by-government-over-growth-concerns-13293755

[24]See Financial Times, *New approach to data is a great opportunity for the UK post-Brexit*, at: https://www.ft.com/content/ac1cbaef-d8bf-49b4-b11d-1fcc96dde0e1

[25]See Open Rights Group, *Cross-party group of MPs warn Govt about unduly influencing Regulator's appointment*, at: https://www.openrightsgroup.org/press-releases/cross-party-group-of-mps-warn-govt-about-unduly-influencing-regulators-appointment/

[26]See The National Data Guardian, at: https://committees.parliament.uk/writtenevidence/121615/pdf/
See also The Biometrics and Surveillance Camera Commissioner, at: https://bills.parliament.uk/publications/51173/documents/3425
See also The Scottish Biometrics and Surveillance Camera Commissioner, at: https://www.biometricscommissioner.scot/news/commissioner-reiterates-concerns-about-data-protection-and-digital-information-no-2-bill-to-scottish-mp-on-westminster-committee/
See also The Equality and Human Rights Commission, at: https://publications.parliament.uk/pa/cm5803/cmpublic/DataProtectionDigitalInformation/memo/DPDIB38.htm

[27]See: https://www.whatdotheyknow.com/request/dpdi_bill

despite the fact that the new Bill drops several provisions of the old DPDI Bill the ICO was previously supportive of.[28]

20. We recommend the House of Commons to retable Amendments HoL125 and HoL126 (Lord Clement-Jones) would remove clauses 91 and 92 of the DUA Bill, thus limiting the Secretary of State powers and leeway to interfere with the objective and impartial functioning of the new Information Commission. Further, w**e recommend the House of Commons to retable amendments HoL127, HoL128 and HoL130 to HoL157 (Lord Clement-Jones)** would modify Schedule 14 of the DPDI Bill to transfer budget responsibility and the appointment process of the non-executive members of the Information Commission to the relevant Select Committee.

21. Transferring the appointment of the members of the Information Commission to the relevant Select Committee would be consistent with the recommendation formulated by Parliament in 2003,[29] 2006,[30] and 2014[31] and, by last, by the Report of the Commission on the UK's Future: A New Britain: Renewing our Democracy and Rebuilding our Economy (so-called Gordon Brown's Report)[32] If so amended, the DUA Bill would ensure that the new Information Commission has sufficient arms-length from the Government to oversee public and private bodies' uses of personal data with impartiality and objectiveness. Strengthening the independence of the ICO would increase the likelihood of the EU granting the UK a data adequacy agreement to the benefit of the UK economy.

4. PROVIDE AN EFFECTIVE AVENUE FOR REDRESS FOR VICTIMS WHOSE COMPLAINTS ARE UNJUSTLY DROPPED BY THE ICO

22. 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

[28]See Information Commissioner's updated response to the Data (Use and Access) (DUA) Bill, at: https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2025/02/information-commissioner-s-updated-response-to-the-data-use-and-access-dua-bill/

[29]See House of Commons Public Administration Select Committee, at: https://publications.parliament.uk/pa/cm200203/cmselect/cmpubadm/165/165.pdf

[30]See Select Committee on Constitutional Affairs, at: https://publications.parliament.uk/pa/cm200506/cmselect/cmconst/991/99109.htm#a22%2044

[31]House of Commons Public Administration Select Committee, Who's accountable? Relationships between Government and arm's-length bodies, at: https://publications.parliament.uk/pa/cm201415/cmselect/cmpubadm/110/11009.htm

[32]See: https://labour.org.uk/wp-content/uploads/2022/12/Commission-on-the-UKs-Future.pdf

because they focus on addressing malpractice and obtaining meaningful changes in how personal data is handled in practice.

23. 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 data protection complaints lodged with them in 2024.[33]

24. As further argued in our statement of support to the amendment to the power of the Commissioner to issue reprimands (supra), that the ICO has consistently been relying on non-binding and highly symbolic enforcement actions to react to serious infringements of the law. Indeed, the Information Commissioner has publicly stated his intention not to rely on effective enforcement against private sector organisations because "fines against big tech companies are ineffective".[34] This opinion has, of course, been widely rebuked by data protection experts and practitioners, including former Information Commissioner Elizabeth Denham.[35]

25. 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 meaningful probe, despite substantiated evidence that Meta's practices do not comply with data protection law.[36] 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.[37]

26. Finally, the current state of affairs means that victims of egregious data protection violations have a greater chance of winning the lottery than finding meaningful redress by complaining to the ICO. This includes, for instance, **victims of Violence Against Women and Girls (VAWG) who have a high need of privacy to protect themselves from abusers and stalkers.**

27. 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,[38] and it was narrowed even further by the

[33]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

[34]https://www.thetimes.com/business-money/companies/article/big-fines-on-tech-companies-are-counter-productive-says-regulator-bfkpc6xrk

[35]https://content.mlex.com/#/content/1614523/eu-s-huge-big-tech-gdpr-fines-don-t-pack-punch-uk-privacy-regulator-says?referrer=search_linkclick

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

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

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

Administrative Court decision which found that the ICO was not obliged to investigate each and every complaint.[39]

28. We recommend the House of Commons to retable amendments HoL18, HoL19, HoL20, HoL22, HoL21, HoL24 and HoL25 (Lord Clement-Jones). These would introduce a new avenue of redress, where complainants could ask the Information Tribunal to review the substance of the Commissioner's response to their complaint. This would allow individuals to promote judicial scrutiny over decisions that have a fundamental impact into how Parliament laws are enforced in practice, and would increase the overall accountability of the new Information Commission.

29. 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[40] and Clearview AI[41] 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 the complaints of 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: if data protection complaints were meant to reduce the imbalance of power between individuals and controllers, this status quo exacerbates this imbalance instead.

30. Furthermore, we recommend the House of Commons to engage with those groups to design and implement stronger legal requirements for complaints handling involving vulnerable groups such as victims of VAWG. These should include a duty to:

- Provide adequate support for vulnerable individuals;
- Hire specialized officers for sensitive cases;

[39]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/

[40]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/

[41]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/

- Improve signposting to support services;
- Implement helpline improvements and de-escalation protocols
- Commit to accountability and immediate action.

5. DO NOT REDUCE ACCOUNTABILITY OVER DATA USES FOR LAW ENFORCEMENT AND PUBLIC SECURITY PURPOSES

31. Schedules 4 and 5 of the DUA Bill would introduce a list of new recognised legitimate interests and compatible purposes. Their effect would be to remove the requirement to consider the legitimate expectations of the individuals whose data is being processed, or the impact this would have on their rights, for the purposes of national security, crime detection and prevention, safeguarding, or answering to a request made by a public authority. Data which is used for the purposes listed in these schedule would not need to undergo either a balancing test under Article 6(1)f, or a compatibility test under Article 6(4), of the UK GDPR.

32. Further, Clause 81 would remove the requirement for police forces to record the reason they are accessing data from a police database.

33. In turn, the combined effect of these provisions would be to authorise a quasi-unconditional data sharing for law enforcement and other public security purposes while, at the same time, reducing accountability and traceability over how the police uses the information they are being shared with. In turn, this risks further eroding trust in law enforcement authorities.

34. We recommend the House of Commons to retable amendments HoL 43, HoL44 and HoL63 (Lord Clement-Jones). This would remove, respectively, Schedule 4, Schedule 5 and Clause 81 of the Data Access and Use Bill. This would ensure that accountability for access to data for law enforcement purposes is not lowered and remains underpinned by a robust test to ensure individuals' rights and expectations are not disproportionately impacted.

35. The public need more, not less transparency and accountability over how, why and when police staff and officers access and use records about them. Just last month, the Met Police admitted that it investigated over 100 staff over the inappropriate accessing of information in relation to Sarah Everard. This shows the police can and do act to access information inappropriately.[42] This is likely the tip of the ice-berg. There may be less prominent cases, where police abuse their power by accessing information without worry for the consequences.

[42]See https://www.bbc.com/news/articles/c8dm0y33yrmo

6. DO NOT ALLOW THE GOVERNMENT TO OVERRIDE KEY ASPECTS OF DATA PROTECTION LAW WITH STATUTORY INSTRUMENTS

36. The Data Use and Access Bill introduces several clauses that would allow the Secretary of State to override primary legislation and modify key aspects of UK data protection law via Statutory Instrument. These include powers to:

- Introduce new legal bases for processing, known as "recognised legitimate interests" (Clause 70).
- Introduce exemptions to the purpose limitation principle, known as "list of compatible purposes" (Clause 71).

37. The list of recognised legitimate interests and compatible purposes introduced by Schedule 4 and Schedule 5 already show the dangerousness of the new powers of the Secretary of State. These Henry VIII clauses are flawed by design:

- **These powers provide wide discretion to the Secretary of State without meaningful parliamentary scrutiny.** Indeed, "no SI has been rejected by the House of Commons since 1979".[43]
- **These powers are being introduced in the absence of a meaningful justification.** While the new Minister has opted not to express their views on this matter, the previous government argued that these powers were meant to allow Ministers to intervene if legislation was interpreted by the Courts in a way the government did not agree with. This is a faulty and dysfunctional rationale, that denies Parliament of its main prerogative—to write the laws that are meant to constrain what the government can do. Such a power can also be easily misused to interfere with, and bypass, a Judicial Review whose outcome the government does not like.
- **Henry VIII powers will, in the words of the House of Lords, "make it harder for Parliament to scrutinise the policy aims of the bill and can raise concerns about legal certainty".[44]** Further, Henry VIII powers should, in the words of the same report, "be recognised as constitutionally anomalous", and their use acceptable "only where there is an exceptional justification and no other realistic way of ensuring effective governance". None of these issues seem to have been addressed by the Data (Use and Access) Bill, where the breadth of the powers it confers does inherently reduce legal certainty and Parliament's ability to scrutinise legislation.
- **These powers were identified by the EU stakeholders as a main source of concern regarding the continuation of the UK adequacy decision, whose review is due in 2025.** The House of Lords inquiry into UK adequacy concluded

[43]The Hansard Society, *Delegated legislation: the problems with the process*, p.16, at: https://www.hansardsociety.org.uk/publications/reports/delegated-legislation-the-problems-with-the-process

[44]Delegated Powers and Regulatory Reform Committee, *Democracy Denied? The urgent need to rebalance power between Parliament and the Executive*, at: https://publications.parliament.uk/pa/ld5802/ldselect/lddelreg/106/10602.htm

that "lawful bases for data processing and the ability to designate legitimate interests by secondary legislation made by Ministers" constituted a significant concern for EU stakeholders and the continuation of the UK adequacy decision.[45] Henry VIII powers were also identified by the European Parliament review of the EU-UK Trade and Cooperation Agreement as a potential barrier to the functioning of such agreement.[46]

- **The risk these powers constitute to the UK adequacy decision are more than hypothetical:** for instance, if these powers were to be used, at any time, to authorise personal data transfers to a country that does not enjoy adequacy status from the EU, or to restrict the definition of special category data, this would guarantee the revocation or annulment of the UK adequacy status.
- **These Powers could be used to undermine the integrity of our elections.** As ORG warns in our latest report 'Moral Hazard, Voter Data Privacy And Politics in Election Canvassing Apps'[47] any party in power could change the rules around how electoral data is used just months before an election takes place. Opposition parties might worry Labour (whose election database runs on Experian, the credit agency servers) might use these powers to obtain even more access to commercial data. Whereas Labour members of Parliament should consider how the laws they are passing could be used by a future Government. Clearly laws on how parties use data should be set in primary legislation not open to Ministerial regulation via SI.
- **These Powers could be used to justify a US-style mass seizure of government data by an unconstitutional agency like DOGE.** Whereas DOGE's misappropriation of government datasets is being successfully challenged in the US on privacy law grounds, a "rogue" UK government would only need to lay Statutory Instruments that authorise the illegal appropriation of government data to make their misuse legal. This severely weakens UK data protection law's ability to protect the public during the event of a constitutional crisis, thus making it easier for a coup d'etat to suceed.

38. We recommend the House of Commons to retable Amendments HoL41 and HoL61 (Lord Clement-Jones). These would remove delegated legislative powers that reduce legal certainty, and allow governments to change primary legislation according to the politics of the day. It would also remove significant risks for the retaining of the UK adequacy status.

[45]Lord Ricketts, *Letter to Rt Hon Peter Kyle MP re: UK-EU data adequacy*, at: https://committees.parliament.uk/publications/45388/documents/225096/default/

[46]OPINION OF THE COMMITTEE ON CIVIL LIBERTIES, JUSTICE AND HOME AFFAIRS (10.10.2023) within *REPORT on the implementation of the EU-UK Trade and Cooperation Agreement*, at: https://www.europarl.europa.eu/doceo/document/A-9-2023-0331_EN.html#_section11

[47]Moral Hazard, Voter Data Privacy And Politics in Election Canvassing Apps **Error! Hyperlink reference not valid.**

7. PROTECT GROW BY ADDRESSING THE THREATS TO THE UK ADEQUACY STATUS

39. Issues we have described in section 1 (automated decision making and AI), section 3 (powers of the Secretary of State), section 4 (use of data for law enforcement and national security purposes) and section 5 (performance and independence of the ICO) have been repeatedly raised by EU stakeholders during the debate of the DPDI Bill, as well as by the UK inquiry into UK adequacy. To summarise:

- Members of the European Parliament have raised issues concerning the powers of the Secretary of State to introduce recognised legitimate interests, the lowering of the right not to be subject to automated-decision-making, and the independence of the ICO.[48] The European Commission responded to that written question, sharing the concerns expressed by the MEPs.[49]
- Members of the European Parliament also raised issues concerning the removal of oversight of biometric data under the DPDI Bill, and the potential impact on the EU-UK Trade and Cooperation Agreement.[50] The Commission responded to the question by emphasising the need of independent oversight of biometric data.[51] While the abolition of the Biometrics Camera Commission is averted by the DUA Bill, the issues surrounding the independence of the ICO remain.
- The European Parliament Committee for Civil Liberties, Justice and Home Affairs (LIBE) wrote to the European Commission to express concerns surrounding the independence of the ICO.[52] The European Commission responded to that letter, haring the concerns expressed by the Chair of the Committee.[53]
- The European Parliament Report on the Implementation of the EU-UK Trade and Cooperation Agreement raised issues concerning the powers of the Secretary of State to introduce recognised legitimate interests, the lowering of the right not to be subject to automated-decision-making, the independence of the ICO and its performance, in particular by emphasising "that the UK data protection supervisory authority has found multiple instances of enforcement failures and that its statistics show very low rates of hard enforcement" and that "rules must be enforced and individuals must have access to an effective complaints procedure".[54]
- The European Parliament Committee for Civil Liberties, Justice and Home Affairs (LIBE) answered to the House of Lords inquiry into UK adequacy,

[48]See: https://www.europarl.europa.eu/doceo/document/E-9-2023-001790_EN.html
[49]See: https://www.europarl.europa.eu/doceo/document/E-9-2023-001790-ASW_EN.html
[50]See: https://www.europarl.europa.eu/doceo/document/E-9-2024-000591_EN.html
[51]See: https://www.europarl.europa.eu/doceo/document/E-9-2024-000591-ASW_EN.html
[52]See: https://www.openrightsgroup.org/publications/8-march-2024-letter-to-commissioner-reynders-from-libe-committee-chair-dpdi-bill/
[53]See: https://www.openrightsgroup.org/publications/28-august-2023-reply-from-commissioner-reynders-to-libe-committee-chair-dpdi-bill/
[54]See: https://www.europarl.europa.eu/doceo/document/A-9-2023-0331_EN.html#_section11

reiterating the concerns expressed above.[55] The Lords' inquiry has recognised the validity of these concerns.[56]

40. Against this background, the DUA Bill takes the important step of removing provisions that would have abolished the Office of the Biometrics and Surveillance Camera Commissioner. On the other hand, however, the Bill would still provide unaccountable delegated legislative powers to Ministers (see above, section 3), broad exemptions to key data protection principles for national security, law enforcement and access to data by public authorities (see above, section 4), and leaves the issue of the independence and performance of the ICO unaddressed (see above, section 5).

41. In a recent institutional visit to the EU, Open Rights Group has heard concerns from EU stakeholders concerning the persistence of these issues in the new Data (Use and Access) Bill. We expect these issues to be raised in public in the upcoming months.

42. 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.[57] 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.

[55]See: https://committees.parliament.uk/writtenevidence/129913/html/

[56]See: https://committees.parliament.uk/publications/45388/documents/225096/default/

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