DUA BILL: ORG STATEMENTS OF SUPPORT AND RATIONALE

Author: Mariano delli Santi

December 2024

In this paper

ICO statutory duty – statement of support for amendment HoL122

HoL122: LORD CLEMENT-JONES

This amendment removes the secondary objectives introduced by the Data Use and Access Bill, which frame innovation, competition, crime prevention and national security as competing objectives against the enforcement of data protection law.

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.

Strong, effective and objective 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.

However, Clause 90 builds on the false 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.[1]
- 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*"[2]. 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"[3] as indicators for regulators to ensure they are delivering competition benefits

Amendment HoL122 would amend Clause 90 and clarify the role and statutory objective of the Information Commissioner's Office by removing unnecessary and potentially counterproductive objectives. This would clearly state 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,[4] such as the ICO.

---

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

2 https://www.gov.uk/government/publications/growth-duty PDF p.7

3 Ibid, p.16

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

ICO reprimands – statement of support for amendment HoL 123

HoL123: LORD CLEMENT-JONES
This amendment ensures that the Commissioner cannot over-rely on reprimands by limiting its powers to issuing only one to a given controller over a fixed period.

The performance of the Information Commissioner's Office has been far from satisfactory. In 2021-22 it did not serve a single GDPR enforcement notice, secured no criminal convictions and issued only four GDPR fines totalling just £633k,[5] despite the fact that it received over 40,000 data subject complaints.[6] 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".

In contrast, the ICO issued "28 reprimands to the public sector over the last financial year".[7] 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:[8]

- 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.[9] 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.[10]

---

5 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

6 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

7 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/

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

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

- 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.[11]
- Two police authorities, Sussex Police and Surrey Police, recorded the conversations of hundreds of thousands of individuals without their consent.[12]
- 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.[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,[14] recording and publishing conversations with Windrush victims without consent,[15] and a systemic failure to answer to SARs within statutory limits, with over 22,000 requests handled late.[16] Against this background, the ICO issued yet another reprimand to the Home Office in 2024.[17] **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.**

Amendment HoL123 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.

---

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

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

12 See https://ico.org.uk/action-weve-taken/enforcement/sussex-police/

13 ICO Alternative Annual Report, p. 14

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

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

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

17 https://ico.org.uk/action-weve-taken/enforcement/home-office/

ICO independence – statement of support for amendments HoL125, HoL126, HoL127, HoL 128, HoL130 to HoL157

HoL125: LORD CLEMENT-JONES
Lord Clement-Jones gives notice of his intention to oppose the Question that Clause 91 stand part of the Bill.

HoL126: LORD CLEMENT-JONES
Lord Clement-Jones gives notice of his intention to oppose the Question that Clause 92 stand part of the Bill.

HoL127, 128, HoL130 to HoL157: LORD CLEMENT-JONES
This amendment and others in the name of Lord Clement-Jones to Schedule 14 remove the involvement of the Secretary of State with the functions of the Commissioner and transfers the responsibility to appoint the Commissioner from government to parliament.

The Data Access and Use Bill would provide significant 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).

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. However, 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.[18] 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".[19]

18 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

19 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/

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.[20]

On top of that, 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.[21] Finally, the Information Commissioner has, once again, welcomed and fully supports the new Data Access and Use Bill, despite the fact that the new Bill drops several provisions of the old DPDI Bill the ICO was previously supportive of.

These events summarised above show two things. On the one hand, the previous Government was able to use the appointment of the new Information Commissioner to align the ICO functioning with their deregulatory agenda and policy objectives without seeking Parliamentary approval. On the other hand, the Information Commissioner's opinion seem to always be aligned with that of the Government of the day, thus failing his responsibilities to provide objective and constructive feedback to Government's policies

Amendments HoL125 and HoL126 would remove clauses 91 and 92 of the Data Acces and Use Bill, thus limiting the Secretary of State powers and leeway to interfere with the objective and impartial functioning of the new Information Commission. Further, **amendments HoL127, HoL128 and HoL130 to HoL157** would modify Schedule 14 of the DPDI Bill to transfer budget responsibility and the appointment process of

20 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

21 See: https://www.whatdotheyknow.com/request/dpdi_bill

the non-executive members of the Information Commission to the relevant Select Committee.

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.

ICO accountability and complaints handling – statement of support for amendments HoL18, HoL19, HoL20, HoL22, HoL21, HoL24, HoL25

HoL18, HoL19, HoL20, HoL22, HoL21, HoL24: LORD CLEMENT-JONES
This new Clause seeks to address the jurisdictional confusion in the 2018 Act, in addition to the new Clause (Transfer of jurisdiction of courts to tribunals).

HoL25: LORD CLEMENT-JONES
This new Clause allows the Lord Chancellor to make Tribunal Procedure Rules instead of the Tribunal Procedure Committee for the purposes of the new Clause (Transfer of jurisdiction of courts to tribunals) for the first time, to allow expedition and flexibility.

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 even where it has ascertained that a violation of data protection law has happened.[22] 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".[23] This

22 See, for instance, Chapter 3 of Open Rights Group, ICO Alternative Annual Report 23-24, at: https://www.openrightsgroup.org/app/uploads/2024/11/Alternative-ICO-Annual-Report-Nov-2024.pdf

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

opinion has, of course, been widely rebuked by data protection experts and practitioners, including former Information Commissioner Elizabeth Denham.[24]

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.[25] 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.[26]

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,[27] 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.[28]

Amendments HoL18, HoL19, HoL20, HoL22, HoL21, HoL24 and HoL25 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.

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

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

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

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

28 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/

Accountability over data uses for law enforcement and public security purposes – statement of support for HoL43, HoL44, HoL63

HoL43: LORD CLEMENT-JONES
This amendment seeks to restore accountability over how data is shared and accessed for law enforcement and other public security purposes.

HoL44: LORD CLEMENT-JONES
This amendment seeks to restore accountability over how data is shared and accessed for law enforcement and other public security purposes.

HoL63: LORD CLEMENT-JONES
This seeks to retain the requirement for police forces to record the reason they are accessing data from a police database.

Schedules 4 and 5 of the Data (Use and Access) 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.

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

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.

Amendments HoL 43, HoL44 and HoL63 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.

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.[29] 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.

Powers of the Secretary of State – statement of support for amendments HoL41 and HoL61

HoL41: LORD CLEMENT-JONES
This amendment deletes powers for Secretary of State to override primary legislation and modify key aspects of UK data protection law via Statutory Instrument.

HoL61: LORD CLEMENT-JONES
This amendment removes powers for Secretary of State to override primary legislation and modify key aspects of UK data protection law via statutory instrument.

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).

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".[30]
- **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

29 See https://www.bbc.com/news/articles/c8dm0y33yrmo

30 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

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".**[31] 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 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.[32] 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.[33]
- **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.

Amendments HoL41 and HoL61 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.

---

31 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

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

33 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