Evidence submission from Dr C.N.M. Pounder[1], Amberhawk Training Limited[2], concerning the data protection elements of ***the Data Use and Access Bill (DUAB)*** (February 2025)

The following is a summary list of nineteen DUAB provisions which act to the detriment of data subjects; the text is intended to assist Committee Members to ask pertinent questions during their debates. I have also suggested possible "***Actions***", where amendments can be developed if Members of the Committee think this is appropriate. I can provide further information if required.

List of problem areas and suggested actions

1. DUAB provides Ministerial powers that deem certain processing to always be lawful (via ***Recognised Legitimate Interests***) and compatible with the purpose of obtaining (listed in Annexes 1 and 2 as introduced into the UK_GDPR). These last two powers we deemed to be excessive and unnecessary by the House of Lords Delegated Powers and Regulatory Reform Committee (9th Report of Session 2024–25, HL Paper 49: 28 November 2024).

In summary, Paragraph 1 of Annex 1 provides for unrestricted voluntary data sharing to any public body for any of its public tasks; the remaining purposes listed in Annexes 1 and 2 already covered by Article 6(1)(f), or the exemptions in Schedules 2 to 5 of DPA2018, or a combination of both. Further detail can be found: "***DUAB makes function creep in the public sector inevitable and lawful***"[3].

These provisions also undermine Parliamentary approval of statutory data sharing powers. Paragraph 1 of Annex 1 provides an alternative pathway to the use of powers to demand personal data which Parliament has already approved. Many public bodies (e.g. HMRC; DWP) can either demand personal data via their many powers, or ask for the same personal data under the new voluntary pathway DUAB provides. The latter approach, if successful, negates the requirement for any statutory protection that Parliament has imposed for such mandatory disclosures. (See paragraph 6 in relation to a similar problem with national security agencies).

[1] Details about my data protection expertise (45 years) can be found on https://amberhawk.com/wp-content/uploads/2022/11/CV-Chris-Pounder.pdf

[2] www.amberhawk.com for details of what Amberhawk Training Limited does.

[3] https://amberhawk.typepad.com/amberhawk/2024/12/duab-makes-function-creep-in-the-public-sector-inevitable-and-lawful.html (Hawktalk blog; December 2024)

Action: The provisions in Clause 70 and 71 and both Annexes 1 and 2 should be removed especially paragraph 1 of Annex 1 and Annex 2. DUAB should specify that public bodies should use their statutory powers as Parliament intended before inviting voluntary disclosure.

2. DUAB provides Ministerial powers that negates the right not to subject to automated decisions; it significantly degrades the protection afforded to data subjects when AI uses ordinary personal data to make automated decisions about them (new A.22D). Having a human review of an automated decision is not a safeguard as the human reviewer will usually confirm the automated decision; it does not remove any central unfairness in the decision.

Informing data subjects about the automated decision is not a safeguard if the data subject has no choice but to submit to such a decision.

The time to legislate for removal of the A.22 right is when one has actual experience of AI automated decision making; not **before** such decision making occurs; the Government has abandoned the Precautionary Principle here. As explained below (see paragraph 7 below), it could take up to 6 months to contest an automated decision with the ICO.

Action: All Article 22 modifications should be subject to a commencement provision when there has been **actual** and **substantial** experience of automated decision making using AI. The ICO can update Parliament on this issue prior to commencement.

3. DUAB provides Ministerial powers to specify high tech firms outside the UK (i.e. established in a Third Country) as offering an adequate level of data protection even though the Third Country itself is not deemed to be adequate (new Article 45A(4)(c)(ii)). Ministers can, via negative resolution, specify for example, "*Palantir in the USA is adequate to process NHS records*" whilst the USA itself is not adequate. These powers are excessive, especially as these kinds of transfer can be subject to the ICO's standard contract clauses instead.

The expansive powers in Schedule 7 that replace the transfer provisions in the UK_GDPR create a risk to the Adequacy Decision with the European Commission because the UK and Commission can significantly diverge on their assessment of the level of data protection in a Third Country.

Action: all Schedule 7 transfer arrangements should be removed. At the very least, the negative affirmative procedures should be replaced by the positive affirmative procedure.

4. The national security agencies (MI5, MI6 & GCHQ) are protected from the DPA2018 because the ICO cannot use his enforcement powers (see section 110, DPA2018); the leaves these agencies outside the scope of enforceable data protection rules.

Instead of no enforcement, actual enforcing of data protection obligations for national security purposes can be transferred to the Investigatory Powers Commissioner. This would help reassure the public that as government expands the meaning of national security (as it has indicated in

the context of illegal immigration), that Part 4 of the DPA2018 and its enforcement provisions apply to such processing (rather than they don't apply – the current situation).

Action: instead of removing the ICO from any enforcement of national security processing of personal data, a simple modification to Section 110 of DPA2018 should transfer responsibility for data protection enforcement to the Investigatory Powers Commissioner (who has the requisite security clearance to investigate complaints).

5. Because of the wide range of the Section 110 exemption (discussed immediately above), it is rather pointless having the ICO having any responsibility for looking at any designation notice (Clauses 82A to 82E). The impact of designation is to transfer personal databases from police control which **is enforced** by the ICO (Part 3 of the DPA2018) to the control of national security agencies (Part 4 of the DPA2018) which **is not enforced** by the ICO.

Action: To be consistent, responsibility concerning consultation/supervision of the designation process should also be transferred from the ICO to the Investigatory Powers Commissioner.

6. The Investigatory Powers Commissioner should be tasked with inquiring whether the exemption in Sections 26 to 28 of DPA2018 (this applies to the voluntary arrangements for disclosure of personal data, from a controller subject to the UK_GDPR, to the national security agencies) overlap with the bulk data sharing provisions in the Investigatory Powers Act 2016. This is to reassure the public that there is no "*back door*" method of bulk dataset collection. In DUAB, for instance, an ANPR database held by the police can be designated for transfer to the national security agencies (see also paras 4 and 5 above for other problems).

With bulk data collection by these national security agencies, there is now a statutory route (Investigatory Powers Act) and a voluntary route (DUAB and DPA2018) where one route is subject to statutory protection and the other is not (exactly like paragraph 1 above).

It is noteworthy that these agencies have a track record of using powers enacted decades earlier for their personal data collections. See "**Section 94 of the Telecommunications Act 1984: a warning from history"**[4] That is why reassurance is required.

Action: the Investigatory Powers Commissioner should be tasked in his Annual Report to include a section on how the national security agencies comply with the provisions in Part 4 (DPA2018).

7. When the data subject complains to the ICO, the ICO expects the complainant to have exhausted the controller's complaint resolution procedures. DUAB formalises this step and introduces at least a 30 day delay before data subjects can complain to the ICO (New sections 164A(3) and

[4] https://amberhawk.typepad.com/amberhawk/2015/11/section-94-of-the-telecommunications-act-1984-a-warning-from-history.html (Hawktalk blog; November 2015)

164A(4)). Note that the 30 day limit relates to acknowledging the complaint and not its resolution; resolving the complaint is associated with a further unspecified time.

Suppose an A.22 complainant writes to the controller about an automated processing decision. Thirty days after that decision, the data subject gets an acknowledgement and then, after an unspecified time, the outcome of the appeal. Only then will there be an approach to the ICO who usually takes 4 to 6 months to form a view. Faced with this six month delay, many data subjects won't bother complaining to the ICO about the automated decision (or about anything else). I suspect that this will be the same for many complaints about controllers.

Action: Exclude A.22 automated decisions from Clause 164A proposals **and** ensure that the 30 days limit relates to resolution of the complaint, not the fact that a complaint has been received.

8. The exemption for scientific research (RAS) purposes introduced by new A.13(5) to A.13(7) and A.14(4) to A.14(6) (right to be informed) does not follow the implementation of exceptions from rights via the usual GDPR mechanisms specified in A.23. The definition of scientific research includes some AI development functionality.

Additionally, the "***appropriate safeguards***" which support this exemption are demonstrably unreliable (e.g. they undermine the Data Minimisation Principle). The exemption also includes the fact that RAS processing is always compatible and disclosures to Third Parties for RAS purposes can be subject to an exemption from transparency (even when personal data are transferred to a Third Party outside the UK).

It does not matter what the nature of the research or AI purpose is. Full details can be found in ***Data Bill legislates for expansive degradation of data subject protection*** [5]

Action: Remove the exemption from A.13 and A.14; the SoS should be told that he has powers to reintroduce it via A.23(1)(e).

9. DUAB places too much power in the SoS to determine regulatory priorities. In addition, the Information Commission should report to Parliament, not a Government Department (DSIT). Two previous Select Committee had previously recommended that the Information Commissioner become directly responsible to, and be funded by, Parliament to protect the independence of the role[6].

[5] https://amberhawk.typepad.com/amberhawk/2025/02/data-bill-legislates-for-expansive-degradation-of-data-subject-protection.html (Hawktalk blog; February 2025)

[6] See, for example, paragraph 10 of https://publications.parliament.uk/pa/cm200809/cmselect/cmjust/146/14604.htm

Action: The subject of who the ICO should report to should be raised again, perhaps as part of a "*should Schedule 14 of DUAB form part of the Bill*" debate

10. Data Protection law is integrally linked to the Human Rights regime via Article 8 ECHR (and to some extent Article 10 ECHR). The ICO is identified in *the Economic Growth (Regulatory Functions) Order 2017* as having to apply economic considerations when deciding to enforce data protection, but the Equality and Human Rights Commission has none for Articles 8 and 10. The inclusion of economic considerations is likely to lead to inconsistent enforcement of Articles 5,6,9,23 and Schedule 1 by the ICO which are linked to A.8 ECHR.

The lack of any discussion on the Growth Regulations as applied to the ICO is described from the middle of: "***Ministers want to pull the strings and rein-in the ICO's independence***"[7]

Action: Modify the list of regulators in *The Economic Growth (Regulatory Functions) Order 2017* to exclude the ICO. Allow data subjects to complain to the Equality and Human Rights Commission concerning breaches of Article 8 ECHR instead of the ICO (as the inclusion of economic factors makes the ICO is an unreliable custodian of A.8 rights; as also described paragraphs 11, 12 and 13 below).

11. All the voting members of the new Information Commission are appointed by the Secretary of State (SoS). This gives too much control to the SoS. so there should be more independence in the appointment mechanism. Some appointees, for example, could be from a privacy NGO tasked with looking after the interests of data subjects.

See my comments on the same provisions that appeared in the DPDI Bill: "***Cronyism at the Information Commission can undermine its regulatory-independence***"[8].

Action: at the very least, ensure that one appointee has the specific responsibility of protecting the interests of data subjects. This idea originates from the DPA1984 when one member of the Tribunal looked after the interests of data subjects and one the interests of controllers.

12. All Codes of Practice or Codes of Conduct specified in the DPA2018, or parts of Codes, relating to data protection compliance should be independently approved by the Information Commissioner. This is because all Ministers head a Government Department which is also a large controller; this in turn means the Minister have a vested interest in the outcome of the processing of personal data and what the Code recommends.

[7] https://amberhawk.typepad.com/amberhawk/2021/11/ministers-want-to-pull-the-strings-and-rein-in-the-icos-independence.html (Hawktalk blog; November 2021)

[8] https://amberhawk.typepad.com/amberhawk/2023/10/cronyism-at-the-information-commission-can-undermine-its-regulatory-independence.html. (Hawktalk blog; Oct. 2023

Ministerial decisions about the content of Codes of Practice that impact on their Departmental responsibilities presents a conflict of interest, and carry an inherent risk of bias against data subjects.

See my comments on the same provisions that appeared in the DPDI Bill: ***DPDI Codes of Conduct allow competent authorities to write their own DP rules***[9] and ***DPDI Bill's Codes of Practice are institutionally biased in favour of controllers***[10]***.***

Action: any Code of Practice or Code of Conduct dealing with data protection have to seek prior approval of the ICO before it becomes operational; this includes Codes under the Digital Economy Act 2017. There will be a need for the ICO to suggest changes to a Code or revoke a Code. There can be consultation with the SoS. If the SoS disagrees with an ICO approved Code, then he should have the power to ask Parliament to vote down the Code.

13. The current Commissioner is reluctant to use his fining powers. This creates a problem with respect to enforcement, because if data protection law is not enforced, it encourages controllers to ignore its provisions. The ICO is clearly of the view that fines do not work (e.g. in the public sector) and, if this view is correct, an alternative enforcement mechanism is needed. In short, the Commissioner has not followed what the law, as enacted by Parliament, requires him to do.

Parliament should thus consider whether, as an alternative, the deliberate misuse of personal data contrary to the data protection rules is a criminal offence (subject to the Proceeds of Crime Act 2002 when large multi-million profits for unlawful processing of personal data can be recovered). Such recovery could provide an alternative to the current fining arrangements involving fines of over £1 million.

This can be achieved quickly by reverting to the DPA1998 and DPA1984 where non-compliance with an Enforcement Notice was an offence committed by the controller; the DPA2018 says such a breach should be a fine (which is not actioned by the ICO).

A controller related offence creates some equity. For instance, employees when they deliberately set out to flout the controller's data protection procedures commit an offence (see section 170 DPA2018). Controllers do not commit an offence if they set out deliberately flout the data protection rules (e.g. Principles and Rights).

Action: Require the Government to hold a swift public consultation as to what is the best way for the ICO to enforce the data protection regime.

---

[9] https://amberhawk.typepad.com/amberhawk/2024/04/dpdi-codes-of-conduct-allow-competent-authorities-to-write-their-own-dp-rules.html (Hawktalk blog; April 2024)

[10] https://amberhawk.typepad.com/amberhawk/2023/08/dpdi-bills-codes-of-practice-are-institutionally-biased-in-favour-of-controllers.html (Hawktalk blog; August 2023)

14. As the ICO is unwilling to use his enforcement powers, then there is a serious risk that controllers will not take their data protection responsibilities seriously. NGOs should be freed to act to pick up some of the slack when the ICO usually decides not to act (e.g. on complaints).

This can be achieved using powers under Article 80(2) when "*the Secretary of State] may provide that anybody, organisation or association [e.g*. a privacy NGO*]…., **independently of a data subject's mandate**, has the right to lodge a complaint with the Commissioner 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" (*my emphasis*).*

Action: To compensate for ICO inaction, the Committee can require the Government to allow Privacy NGOs to take independent action to protect data subjects.

15. There should be a mechanism whereby data subjects can use the Tribunal system when there is a failure of the Commissioner to act on a complaint. This is especially the case when the ICO, as a matter of policy, has decided not to enforce the data protection regime.

There is ample evidence that the ICO has made mistakes in his decision making process and has failed to take action; in some cases he has written to data subjects telling them to apply to the Courts for relief. The Tribunal cannot review the ICO's decisions not to act and the only recourse for the data subject is Judicial Review of the ICO's decision. In relation to rights, data subjects can apply to the Courts for a Compliance Order. Both are costly processes for all concerned.

Under the FOI regime, the ICO decision not to release requested information can be challenged; under data protection, the ICO's failure to require a controller to provide personal data on subject access cannot.

Additionally, the ICO prefers to enforce the UK_GDPR via "reprimands" of controllers. There is no appeal against a reprimand apart from Judicial Review, and to some extent the lack of an Appeal is unfair to Controllers who are often faced with the attendant bad publicity.

Action: there should be a data subject appeal to the Tribunal that the ICO failed to act. This has to be restricted to reduce the risk of flippant appeals from disgruntled data subjects. So the data subject's grounds of an appeal to the Tribunal has to, for example, present a data protection issue of public interest that need resolution. If successful the Tribunal could force the ICO to review the ICO's failure to act.

16. With respect to the processing of personal data for marketing, direct marketing on behalf of a controller or Third Party should **not** be legitimised in terms of *legitimate interests* in all circumstances. DUAB overturns a 35 years-old data protection standard that Third Party marketing requires consent (i.e. since the Linguaphone Decision under the DPA1984).

See the **Appendix** on page 10 which shows an extract of the ICO's guidance direct marketing and the data protection standards that prevailed under the DPA1998 (which are being overturned).

Many company email addresses for staff are of the form name@organisation.co..uk (e.g. MPname@parliament.uk). These can be scraped of the Internet and used indiscriminately for spam for marketing purposes via "*legitimate interests*" provisions in DUAB (new Article 6, paragraph 11(a)). This use of "*legitimate interests"* risks creating a spammer's charter.

Further detail which relate to the similar provisions in the previous DPDI Bill can be found on my blog: ***DPDI No.2 Bill dumps all data subject consent requirements for Third Party marketing***:[11]

Action: Article 6, paragraph 11(a) (Clause 70) should be amended to limit *legitimate interests* to be used in exceptional circumstances where the established DPA1998 consent standard for such marketing is impractical.

17. DUAB fails to correct the non-implementation of the ECHR Judgement in the case of ***Gaskin v UK*** *(1989) 12 EHRR 36.* I have included this as the Adequacy Agreement with the European Commission assumes Strasbourg Jurisprudence on the ECHR/data protection is followed by the UK, and this is an example where it isn't. Such non-compliance is a red-line for the Commission.

Details of the *Gaskin* case as it applies to data protection can be seen under the heading "***Confidential References exemption (DPA1998)"*** [12] (in the middle of the text).

Action: Change the exemption in Schedule 2, paragraph 24 of the DPA2018 so it only applies to the sender of the confidential reference (i.e. return to the position established in the DPA1998).

18. The Ministerial powers to add special category of personal data to the list in A.9(1) UK_GDPR might actually permit (rather than prohibit) the processing of such special data (i.e. the provision might not be a safeguard as touted by the Government). The provision could allow the SoS to introduce sub-classification of existing special category of personal data linked to a particular context or purpose (e.g. on the lines used in the existing "*biometric data for the purpose of uniquely identifying a natural person"*; see A.9(1) UK_GDPR).

For example, a class of special category of personal data such as "*cancer records in the context of training AI algorithms*" would make it easier to process such personal data in accordance with one of the conditions that lifts the prohibition. Thus, far from prohibiting the processing of **new** special category of personal data, the power to add context to **existing** special categories of

---

[11] https://amberhawk.typepad.com/amberhawk/2023/05/dpdi-no2-bill-dumps-all-data-subject-consent-requirements-for-third-party-marketing.html. (Hawktalk blog; May 2023

[12] See from middle of https://amberhawk.typepad.com/amberhawk/2024/12/duab-makes-function-creep-in-the-public-sector-inevitable-and-lawful.html). (Hawktalk blog; December 2024)

personal data could expand the processing of these special categories without the explicit consent of the data subject (the option in A.9(2)(a)).

Action: this point should be explored when the Committee considers whether the relevant clause should stand as part of the Bill.

19. As background to the Government's Digital Verification Identity proposals in Part 2 of DUAB, I refer to the "***Nine Identity Assurance Principles***" that were published in 2015 for inclusion in any future Governmental digital identity project. The Principles were produced by a specialist group of privacy experts (the Privacy and Consumer Advisory Group: PCAG) which included the author; the Principles are still available on the Government website[13]. PCAG was established by the Cabinet Office.

These Principles were originally produced to avoid a repeat of the ID Card debacle a decade earlier; the Government asked a number of privacy experts (including the ICO) to debate and draft a set of objectives so that national ID could become acceptable on data protection grounds.

As a result, these Principles emerged to provide a benchmark for all digital identity schemes. It allows one to identify which Principle is not being considered and the consequences of that lack of consideration. In DUAB, there is no evidence that the Principles have been considered.

It is interesting to note the current successor Committee to PCAG (OLIPAG) was disbanded by DSIT officials in February 2025 as part of the merger of Cabinet Office responsibilities. There were many internal OLIPAG debates concerning One Login: the Government's authentication and identity verification scheme for millions of users.

Further details can be found on:: ***Government's digital identity proposals ignore obvious privacy concerns***.[14]

Action: The ICO should be tasked, as part of his Annual Report, to include a section on how well Part 2 of DUAB performs, including how well the Digital Verification Services including One Login performs with respect to compliance with the Nine Identity Assurance Principles. There should be explicit reference to these Principles in Part 2 of DUAB to reassure the public. They could appear as a Code of Practice under the auspices of the ICO.

[13] https://www.gov.uk/government/publications/govuk-verify-identity-assurance-principles/identity-assurance-principles

[14] https://amberhawk.typepad.com/amberhawk/2023/02/governments-digital-identity-proposals-ignore-obvious-privacy-concerns.html (Hawktalk blog; February 2023)

APPENDIX: Marketing standards of the Data Protection Act 1998

The diagram below is from the ICO's Direct Marketing Guidance (DPA1998).

It can be seen that the ICO recommends "***opt-in consent***" for all electronic marketing and also for third party marketing. By contrast the DUAB permits Third Party and Controller "***opt-out***" by virtue of new Article 6(11)(a). As stated in paragraph 17 above, this change could be a spammers charter.

If one misses an "***opt-out***", one gets marketing; this is not the case with ***"opt-in***". The Government has yet to explain the general reduction of marketing standards, which in my view, could result in irritating spam especially targeted at work email addresses which are not subject to PECR.