Department for Science, Innovation & Technology

Lord Vallance of Balham
Minister of State for Science, Innovation & Technology
Department for Science, Innovation & Technology
100 Parliament Street
London SW1A 2BQ

www.gov.uk/dsit

14 January 2025

House of Lords
London
SW1A 0PW

To: The Baroness Drake CBE, Chair of the Constitution Committee

Dear Lady Drake,

Response to the Report on the Data (Use and Access) Bill

I'm writing to you here to provide you with a detailed response to the report of the Constitution Committee on the Data (Use and Access) Bill ('The Bill'). The Bill completed Lords Committee stage on 18th December 2024 and is now proceeding to Report stage on 21st January 2024.

I want to thank you and the Committee members for your recommendations on the Bill, to which I have responded in detail below. I will also deposit a copy of this letter in the House library.

Clause 28 – Requirement for Secretary of State to prepare and publish a document which sets out the rules concerning the provision of DVS

I note the Committee's continued concerns and hope it will be helpful to offer some background on the role of the trust framework within the certification process for digital verification service (**DVS**) providers, together with an explanation of how and why that framework is underpinned by the measures in Part 2 of the Bill.

Conformity assessment/certification

As clause 33(1)(a) of the Bill makes clear, a prerequisite for applying to the DVS register is that a provider holds a certificate from an accredited conformity assessment body (**CAB)** certifying that they provide digital verification services in accordance with the DVS trust framework.

That conformity assessment is conducted outside of the Bill in accordance with the existing certification system, which explains the limited reference to it therein. The Bill does however set out the definition of an 'accredited conformity assessment body' in clause 33(6) as "*a conformity assessment body that is accredited by the UK national accreditation body in accordance with Article 5 of the Accreditation Regulation as competent to carry out assessments of whether digital verification services are provided in accordance with the DVS trust framework".* The Accreditation Regulation, as noted in clause 33(7), is Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008, which sets out "the requirements for accreditation and market surveillance relating to the marketing of products". The UK national accreditation body is the UK Accreditation Service (**UKAS**).

For the purpose of DVS the Government has therefore created, again outside of the Bill, a 'certification scheme' which defines what conformity assessment bodies have to do in order to certify services against the trust framework. This scheme is based on international best practice, the International Organization Standard ISO/IEC 17065:2012 standard, which sets a clear baseline for how to evaluate products, services and processes and the minimum quality standards that CABs must follow.

UKAS independently reviews the quality of this certification scheme and the DVS trust framework by way of a detailed technical process called 'recognition' to ensure it aligns to international standards and best practice. The non-statutory beta version of the trust framework and its associated certification scheme were first 'recognised' by UKAS in April 2024. Once UKAS 'recognises' the certification scheme, it then 'accredits' CABs, auditing them to check they are implementing the certification scheme correctly.

Once a DVS provider has a certificate, the CABs continue to evaluate the provider's ongoing compliance with the trust framework rules, which includes an at least annual re-evaluation and spot checks. If a CAB finds a 'non-conformity', as independent third parties they are responsible for deciding how to respond. This will normally involve giving the DVS provider time to address the 'non-conformity'. Withdrawal of a certificate is reserved for the most serious of cases. A dispute resolution process provides for areas of disagreement.

There are similar schemes which exist across industries providing quality assurance through the process of conformity assessment and which do not require their rules to be laid before Parliament, noting the previous explanation in the Delegated Powers Memorandum that the trust framework rules in the main draw on and often signpost existing standards, best practice, guidance and legislation.

As also noted in the Delegated Powers Memorandum, like these other schemes, the non-statutory version of the trust framework is currently in operation and dozens of services have already been certified against previous iterations of those rules.

Underpinning the DVS trust framework in legislation

The reason that it was necessary to underpin the conformity assessment process in the Bill is because information sharing powers were needed for the information gateway provided for in clause 45. In order to make clear which DVS providers are entitled to make requests of public authorities under that gateway, the Government decided that a statutory register (the **DVS register**) should be established, access to which is limited to DVS providers with services that are certified as being in compliance with the trust framework rules. The legislation then, as we set out in the Delegated Powers Memorandum, places additional obligations on the Secretary of State regarding consultation in respect of that framework and its review.

Although the Secretary of State does have powers to add and remove DVS providers from the DVS register where he considers they are not complying with the DVS trust framework (or, where relevant, a supplementary code), where they have failed to provide required information, or where there are national security concerns, it is intended that these powers will be used only as a safety net to the conformity assessment process, where, for example, a CAB does not have access to national security information. These powers are of course subject to public law principles and judicial review.

Compliance monitoring against the DVS trust framework will therefore in the main happen as part of the conformity assessment process.

I hope that this background, when read together with the Delegated Powers Memorandum explaining the contents of the DVS trust framework, will provide some helpful context as to the Government remains of the view that it does not require parliamentary scrutiny, because its primary role is in the conformity assessment space which sits outside of the Bill.

Clauses 70(4) and 71(5) - GDPR: Discretion given to Secretary of State to determine and vary the conditions under which personal data can be processed

Clause 70 of the Bill is designed to give commercial organisations and other non-public bodies greater confidence about processing personal data in a narrow range of situations that serve public interest objectives, such as the prevention of crime. Under the current legislation, organisations must do a detailed assessment of whether their interests in processing the data for such purposes are outweighed by the rights and freedoms of data subjects. This is sometimes referred to as a ‘legitimate interests assessment’. ICO guidance recommends that the outcome of such an assessment is documented.

The Government considers that such an assessment should not be required where the processing is necessary and proportionate to prevent crime, safeguard vulnerable people or to fulfil any of the other recognised legitimate interests listed in new Annex 1 to the UK GDPR (as introduced by Schedule 4 to the Bill). In such situations, there may be a need to share personal data quickly to reduce the risk of harm. Requiring organisations to pause to complete the necessary assessments and paperwork could be harmful in such situations.

We recognise the Committee are concerned about provisions in Clause 70 that give the Secretary of State the power to add new activities to the list of 'recognised legitimate interests', or vary the existing provisions, via regulations. The Government has taken steps to limit the types of processing activity that could be added to the list. Before making any changes, the Secretary of State must carefully consider the fundamental rights and freedoms of individuals, particularly ensuring that children's unique vulnerabilities are accounted for, given they may be less aware of the risks associated with data processing. Additionally, any new processing activity being included in the list must be necessary to serve public interest objectives as described in Article 23(1) of the UK GDPR.

To ensure there is appropriate scrutiny of any amendments to the list of recognised legitimate interests, the Secretary of State must consult the Information Commissioner and other interested parties on the development of any regulations. Any regulations must then go through the affirmative resolution procedure, requiring approval by Parliament following a debate in both Houses.

The Government considers that the regulation-making power should be retained in case there is a need to promote swift and decisive data processing in relation to other public interest activities in the future, but it is confident that the requirements and limitations included in the clause will ensure that these powers are used sparingly.

With regard to Clause 71, this concerns the purpose limitation principle in the UK GDPR, notably that personal data must not be further processed in a manner incompatible with the purposes for which it was obtained.

Exceptions to the compatibility requirement may be currently made when the data subject has given consent, or when the processing is based on a law that constitutes a necessary and proportionate measure to safeguard important objectives of public interest. This is particularly important because a new purpose that is substantially different from the original purpose may struggle to pass the compatibility assessment, regardless of being in the public interest.

An example of a current exemption is paragraph 2 of Schedule 2 to the DPA 2018, which covers processing for prevention or detection of crime, the apprehension or prosecution of offenders, or the assessment or collection of a tax or duty or similar imposition. There is currently a power in section 16 of the DPA 2018 to add further exemptions from the purpose limitation principle.

The Government believes the current law on the purpose limitation principle (and exceptions to it) is unclear and hard to navigate or interpret for both controllers and individuals. Clause 71 aims to provide more clarity and certainty around the purpose limitation principle. The clause delineates the routes for compliant further processing, where new purposes are to be treated as compatible with the original purposes. This includes an exhaustive list of public interest situations in Annex 2 of the UK GDPR. As part of this consolidation, the exemption from the purpose limitation (as a result of it being listed in para.1(b)(ii) of Schedule 2 to the DPA 2018) in paragraph 2 of Schedule 2 to the DPA 2018 and others are being relocated to Annex 2. The current power in section 16 of the DPA 2018 mentioned above will no longer be relevant as regards the purpose limitation once this relocation and consolidation has occurred. The power proposed in new Article 8A(5) under Clause 71 is intended to replace it.

The power is strictly limited to objectives listed in Article 23(1) of the UK GDPR. These reflect objectives of public interest, including prevention of crime, enforcement of civil law claims, and protection of the data subject themselves or the rights and freedoms of others. This means that if an intended use of the power is not for an objective in the public interest, it cannot be used. If the intended use does fall under the objectives listed in Article 23(1), then it is vital the Government can quickly react to ensure the processing is not blocked.

The power may be particularly necessary in light of how Clause 71 is creating an explicit restriction on the re-use of data collected under the data subject's consent. While the Government believes this restriction is implicit under the current law, some data controllers may be unaware of it due to the difficulty of interpreting the existing provisions. This raises the risk that there are further processing situations of important public interest that are not currently in Annex 2 but deserve to be.

Finally, in addition to ensuring the list can be up to date, the power is important to be able to narrow the listed situations in Annex 2 if there is evidence of misuse or harm to data subjects. It will ensure action can be swiftly taken to protect data subjects by limiting an exemption or adding further procedural safeguards to it. The same parliamentary and consultation requirements outlined for Clause 70 also apply for exercising this power in Clause 71.

I hope it will reassure the Committee that the power will be used only when necessary and in the public interest.

Clause 105 – Constitutional statutes

The Committee also highlights a point on constitutional statutes and the principle of implied repeal, citing the judgment by Lord Justice Laws in Thoburn in 2002. New section 183A of the Data Protection Act 2018, inserted by clause 105 of the Bill, will create a rebuttable presumption that the data protection legislation will apply for any new duties or powers to process personal data that are created in future legislation.

This provision does not bind future Parliaments, which will have the option of setting the presumption aside when creating new duties or powers to process personal data. The purpose of this presumption is to avoid any doubt arising about whether later legislation has impliedly repealed the UK's data protection legislation. In the future, any new enactments that do not make express provision setting the data protection legislation aside will continue to be read consistently with the data protection legislation.

Clause 133 – A Henry VIII power

As the Committee notes, clause 133 of the Bill confers a power to make amendments consequential on any provision made by the Bill. It is a Henry VIII power drafted to allow the amendment, repeal or revocation of provisions of legislation passed or made before the end of the parliamentary Session in which the Bill is passed.

The power to amend legislation passed or made in the same Session is included because, at the time at which a Bill is introduced, it isn't possible to be certain how its provisions will interact with other Bills introduced in the same Session, or the order in which they will reach the statute book.

For example, a Bill introduced at the beginning of a Session cannot take account of a Bill introduced later in the Session and it might not make sense to draft the Bill introduced later in the Session in a way that takes account of the earlier one as it may not be known which will be enacted first or the sequencing of commencement. We therefore do not think that the Government can be sure that future legislation in the same Session is drafted in a way that is compatible with the Bill.

Extending a consequential amendment power conferred by a Bill to legislation passed or made in the same Session is a well-established technique to address the inherent uncertainty about the order in which Bills in a Session will become law. For example, similar provision was included in the Data Protection Act 2018 (see the definition of "enactment" in s.205(1), which includes legislation passed or made after that Act, and the power to make consequential amendments under s.211(2) to (7), which is restricted to amendments of legislation passed or made before the end of the Session in which that Act was passed).

The Bill already includes consequential changes to primary legislation (including in Chapter 1 of Part 5 of the Data Protection Act 2018), but we cannot be confident that all necessary consequential amendments to legislation have been identified in the Bill's preparation, particularly in relation to other primary legislation that is still going through Parliament in this Session.

This power is limited to making amendments to other legislation that are genuinely consequential on the provisions in this Bill and is therefore relatively narrow in scope.

Further, any amendments to primary legislation will be subject to the affirmative procedure.

Schedule 15 - Information Standards for health and social care

We thank the Committee for their comments and consideration of the constitutional implications of Schedule 15 in the Bill.

We do not consider that a requirement for each information standard to be laid before Parliament for scrutiny would be appropriate or proportionate for four reasons.

Firstly, Information standards are usually technical and reflect international best practice in information technology. Information standards include detailed operational and technical requirements. It is customary for the preparation of such documents to be delegated to the relevant authority. Parliament will have the opportunity to scrutinise the procedure for preparing and publishing information standards to be undertaken by the relevant authority (see third point below).

Secondly, the Health and Care Act 2022 Information Standards procedural regulations, which will set out the procedure to be followed in the preparation and publication of information standards, will – Parliament permitting – ensure information standards have benefited from expert input to ensure they are fit for purpose. DHSC is preparing procedural regulations under the Health and Care Act 2022 (HCA 2022). Parliament permitting, the regulations would include provision that the Secretary of State, or NHS England, should seek advice from other persons when preparing and/or revising an information standard. As a result, information standards will benefit from rounded expert input to ensure they are fit for purpose.

Thirdly, drafting of the procedural regulations has been informed by stakeholder views and these regulations will be subject to parliamentary scrutiny. Under the HCA 2022, the Secretary of State is required to consult such persons as the Secretary of State considers appropriate before laying the procedural regulations. A public consultation was undertaken in 2024 that set out DHSC's proposals for this procedure, and invited views on them. This can be accessed here: Information standards for health and adult social care - GOV.UK.

DHSC intends to lay the draft Regulations in Spring 2025 for scrutiny by Parliament, so that Parliament can consider whether the process is sufficiently robust and effective. These will provide a clear framework for how new information standards will be created. The procedures set out would apply to any future information standards published following commencement of the changes proposed by the DUA Bill.

Fourthly, the scope of information standards is defined on the face of the Bill. The application of information standards is limited to a defined set of persons, and information standards may only be set in relation to information concerning, or connected with, the provision of health care or of adult social care in England.

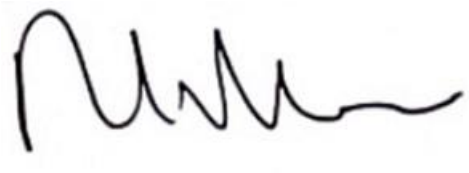
Currently, publicly funded health and adult social care organisations in England must have regard to information standards. Changes made by the HCA 2022 will, once commenced, make information standards mandatory and extend them so that they can apply to Care Quality Commission regulated private health and adult social care

providers. The HCA 2022 also sets out that an information standard must specify to whom it applies.

Changes proposed in the DUA Bill would allow information standards to apply to a “relevant IT provider”: a person involved in information technology, and IT service or a service which consists of processing information using information technology (whether for payment or free of charge) but only in so far as the technology or service is used, or intended to be used, in connection with the provision in, or in relation to, England of health care or of adult social care.

Thank you again for your sustained engagement with this Bill.

Yours sincerely,



Lord Vallance of Balham
Minister of State
Department for Science, Innovation and Technology