

Parliamentary briefing, 4th February 2025

Overview

The government's [Data \(Use and Access\) Bill](#) will soon be moving to the House of Commons, with the second reading expected on 12th February.

The bill provides the legislative framework for **digital verification services** (DVS), which will allow people to prove their identity and facts about themselves by using digital apps and online services, backed by a government “**trustmark**”. The system relies on the trustworthiness of underlying data provided by public authorities such as the DVLA, HM Passport Office and NHS via a new information gateway (without relying on scanning or showing paper documents). **For the system to work, the digital data provided from public sources must be accurate, reliable and clearly defined.**

But there is a problem with these data sources.¹ When it comes to data on sex (whether someone is male or female) up to 100,000 people may have changed the information on some of their records, such as those held

¹ Sex Matters (2024). [Sex and the Data Bill](#).

about them by the DVLA, Passport Office and NHS.² These agencies will change a person's recorded sex on request, and do not keep robust records. This does not relate to the Gender Recognition Act 2004, but has been done by these agencies without any legislation or parliamentary oversight.

Public bodies routinely mix up sex and “gender identity” in the same field, making their data unreliable. This is not in line with data-protection standards.

If the problem of identifying reliable data sources (and excluding unreliable ones) is not solved in relation to the DVS system, the government will be putting a false and unreliable “proof” of sex in everyone's pocket. This will destroy the ability to reliably share and use data about sex, which is crucial for safeguarding, healthcare, single-sex services, sports and collecting demographic data.

A robust system based on accurate data would protect transgender people's rights, because it would ensure that their data is accurate whenever it is needed (such as for healthcare) and that it can be kept private where it is not.

² According to the last censuses in England and Wales and Scotland there are about 100,000 people who identify as a “transgender man” or a “transgender woman” (although there are concerns about the reliability of this data). Only around 8,500 have a gender-recognition certificate (GRC).

An unreliable, ambiguous system will be a costly, wasteful failure. If the government's flagship digital identity service framework "verifies" false information as true it will harm both transgender people, other service users, and service providers, and will result in costly legal challenges and technical failures.

The government's view

The government recognises the important goal that data is accurate and reliable. During the debate on 21st January, Lord Vallance said that:

"The Government believe that ensuring **the data they process is accurate** is essential to deliver services that meet citizens' needs and ensure accurate evaluation and research."

"I can be absolutely clear that **we must have a single version of the truth** on this. There needs to be a way to verify it consistently and there need to be rules."

"I know from my background in scientific research that, **to know what you are dealing with, data is the most important thing to get.** Making sure that we have a system to get this clear will be part of what we are doing."

However, he did not support specific amendments to safeguard the accuracy of data from public authorities, saying instead that the DVS framework would draw "on existing technical requirements, standards, best practice,

guidance and legislation” and rely on public authorities already meeting **data-protection standards**.

It is crucial now that the government recognises the problem with public data sources not following data-protection standards when it comes to sex data.

Closing the loopholes: safeguards in the current bill

During the bill’s progression through the Lords, three safeguards were introduced to close these loopholes and ensure that only reliable data held by public sources is fed into the system.

- **Clause 28** requires that the Secretary of State publish rules for digital verification services (“**the trust framework**”). The bill coming from the House of Lords requires that this includes assessing whether key public authorities collect, record and share personal data attributes reliably.
- **Clause 45** gives public authorities the power to disclose an individual’s personal information to certified DVS service providers at the request of that individual (via “**the information gateway**”). The bill stipulates that a public authority must not disclose information unless it is able to attest that it was accurate at the time it was recorded, and has not been changed or tampered with, other than through a lawfully made correction. The data must be clearly defined and accompanied by metadata.

- **Clause 139** provides that the Secretary of State may make regulations establishing the definitions and associated metadata (descriptions) for core personal data attributes (a “**data dictionary**”) and require that these definitions are used across the DVS system and registers of births and deaths, as well as in other areas including health and social care.

These three safeguards make it the responsibility of the Secretary of State to ensure that digital verification services backed by a government trustmark are designed to provide reliable, trustworthy information, and to give him the tools to do so.

These measures will protect the private-sector service providers that are being invited to invest to build services by ensuring that public bodies are held to the same standards of integrity and reliability as private service providers.

They will protect transgender people who have the same right as everyone else to have their biological sex accurately recorded wherever their biological sex is needed, and to keep their sex private when that information is not needed. They are compatible with the Gender Recognition Act, which already allows for data-sharing with consent.

House of Commons stages

During the next stages of the bill's passage we hope that MPs will raise the issue of unreliable sex data, and the risks that this causes to the integrity of the system and to service users. We hope that the government will grasp the problem and provide specific practical reassurance concerning how it will be addressed, including by referring the issue to the Information Commissioner.

Any amendments to these clauses should not undermine the guarantee of reliable, accurate data.

For more information contact Laura Pascal at Sex Matters: info@sex-matters.org

*Sex Matters is a charitable incorporated organisation
number 1207701*