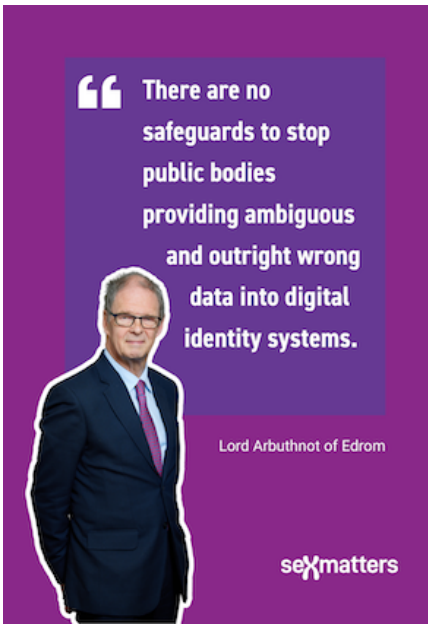
Sex and digital identities

Briefing, June 2025



On 19th June, the Data (Use and Access) Act 2025 (see bills.parliament.uk/bills/3825) received royal assent. The bill created the statutory framework for digital identity services. The aim of these services is to improve people's lives by making transactions simpler and more secure by enabling people to prove facts about themselves digitally. Initial applications include accessing age-restricted products, renting a flat or starting a new job.

During the passage of the bill, concerns were raised in Parliament that digital verification services that pull data from unreliable data sources (such as that held by HM Passport Office) would wrongly "verify" that a person is male or female, instead of accurately verifying their

biological sex where this information is needed (such as for single-sex services, sports, healthcare and jobs where sex matters).

Ministers gave reassurances that this issue will be addressed in the design of the system. As Minister of State, Department for Science, Innovation and Technology, Lord Vallance of Balham said in the House of Lords on 12th May (see Hansard, Data (Use and Access) Bill, 12th May 2025):

> "This Government are clear that data must be accurate for the purpose for which it is being used and must not be misleading. It should be clear to digital verification services what the information public authorities are sharing with them means. I will give an important example. If an organisation needs to know a person's biological sex, this Government are clear that a check cannot be made against passport data, as it does not capture biological sex. DVS could only verify biological sex using data that records that attribute specifically, not data that records sex or gender more widely."

How accuracy and reliability can be achieved simply

The Data (Use and Access) Act 2025 establishes the statutory basis for creating a system of government certified digital verification services, underpinned by:

a) a **code of practice** for public authorities sharing personal data

b) a **trust framework** for certifying private-sector service providers

c) an **information gateway** linking public authority data sources with private-sector providers of verification services.

In order to achieve the stated aim of enabling people to prove facts about themselves simply and efficiently, all these elements must work together to enable automated systems to distinguish between reliable and unreliable datasets. The Office for Digital Identities and Attributes is now finalising the details of these instruments.

To address the legacy problem of datasets that are unreliable in relation to sex, such as those held by the NHS, HMPO and DVLA, the Secretary of State should:

(1) As part of the **code of practice include a requirement for public authorities** to—

(a) **review their datasets** relating to the attribute of sex (which may have been termed “gender”) and identify whether they record:

(i) **”Sex”** defined as being the immutable biological characteristic of being male or female (sometimes called “sex at birth”, “natal sex” or “biological sex”);

(ii) **“Acquired Gender”** meaning male or female by virtue of a gender recognition certificate issued under the Gender Recognition Act 2004

(iii) **Mixed data** which combines sex, acquired gender and/or gender identity data in a single field.

(b) **publish a register of these datasets** and the purpose(s) for which they have been collected and keep it under annual review thereafter

(c) **publish a statement** in a prominent place on their website, alongside the register, and in metadata attached to digital data feeds, identifying any mixed datasets and warning that they cannot be used to verify sex.

(2) **As part of establishing the information gateway,** set up a register of public authorities approved to act as sources of data relating to the attribute of sex for persons providing digital verification services, and **publish the register** on the website of the Office for Digital Identities and Attributes.

(3) **Include in the trust framework** directions that digital verification services may only treat data on sex from public authorities as authoritative if it comes from a source included on the register. Other data from public authorities should not be processed into the sex field. This will include updating the guidance on how to score attributes to include a specific section on how to score data sources in relation to the sex attribute (see Government Digital Service (2021). *How to score attributes*).

What if these steps are not taken?

If the system is implemented without addressing the problem of inaccurate sex data, the government will be launching a system of “trusted digital identity” without crucial safeguards needed to enable trust and accuracy. It will create real harms, such as people who have changed their sex records being flagged up as “synthetic identity” risks because they have mismatched records, and data users unable to rely on the system to provide accurate information where it is needed, such as for keeping people safe in single-sex services and sports.

If action is not taken, the government risks legal challenges, liabilities, financial costs and inefficiencies that could derail the whole digital-identity system.

For more information, see the resources at
sex-matters.org/digital-id
OR contact Laura Pascal at Sex Matters:
PublicAffairs@sex-matters.org