The need for a unifying vision

The Data (Use and Access) Act 2025 (Data Act) gives people what they need in a digital economy: meaningful control over their own data. It translates the principle of individual liberty into digital practice by enabling voluntary digital identity and personal data sovereignty for all.

The consultation on digital ID should therefore set out a clear vision for the UK's regulated private data ecosystem, based on three core principles:

- **Inclusion:** Solutions must be easy for everyone to use including those without passports or driving licences or with limited digital access
- **Trust:** Providers must operate to high standards of assurance, transparency, duty of care and accountability.
- **Control:** Individuals must have the power to decide who can access their data and when in the same way they control access to their money today.

Digital Identity sits at the centre of this vision.

The consultation needs to resolve a deceptively simple question:

Is your identity something you own - or something the state owns?

This distinction matters. You define your identity by what matters to you. The products you buy, the services you use, and what you are entitled to from the state are all conditional - you make a choice and gain access once you share something about yourself. We already understand this transactional idea when we earn and spend money. Now, in our digital future, we can think about collecting and re-sharing our data in the same way.

In this context, a **digital wallet** is like a bank account for your data. A **digital ID**, and the data linked to it, is just one item inside that wallet - one credential among many that you own, and you may even have more than one wallet. Its up to you to decide. You are in control.

Committing to this simple but transformation vision is pivotal. It will shape system design, regulatory responsibility, and investment patterns for decades to come. Delivering it requires creating a personal data ecosystem that mirrors the resilience, security, and choice found in the UK's retail banking, building society, and credit union landscape.

To this end, the privacy community and the Digital Verification Services (DVS) sector are strongly aligned. This not accidental. It reflects the reaction to the National ID Card proposals under the previous Labour Government, which led to the Crosby Review in 2008 on identity assurance. Since then, cross-party consensus has built on these principles, resulting in the Digital Identity and Attributes Framework (DIATF), the establishment of the DVS market, and the Data Act.

By contrast, the current proposals for a GOV.UK Wallet mandate that government-issued credentials will **ONLY** be held in the GOV.UK Wallet, and government will **ONLY** accept credentials it issues itself. This represents a clear departure from the UK's long-standing direction as defined in the Data Act. It is a proposal that was taken without consultation or impact assessment. **This consultation must therefore test, not assume, this proposal.**

It is right that government modernises how people interact with the state, and a GOV.UK Wallet will form part of that journey. But the means matter as much as the ends. This is the design choice to be resolved - *is your identity something you own - or something the state owns?*

In short, this consultation is about the type of digital future we choose to shape together, not just for today but for generations to come.

A Clear Role for the Private Sector

The Data Act provides a simple organising principle to guide this consultation:

Government will issue credentials and set standards; citizens will be free to choose how and where those credentials are held and presented, within an accredited DVS Trust Framework.

This approach, already defined in legislation, supports consumer choice, avoids lock-in, and ensures a resilient system where innovation continues without compromising standards. It defines that all wallets and credentials must:

- operate on equal terms with accredited providers
- accept credentials from all compliant issuers
- avoid creating structural advantages for any single delivery channel

With this as the baseline, the consultation can test two different approaches to a new voluntary government digital identity credential:

1. It sits exclusively within the GOV.UK Wallet (the current proposal).
2. It forms part of the DVS Trust Framework as outlined above.

The consultation must result in a clear and published impact assessment of the GOV.UK Wallet approach, including projected public expenditure, operating costs, expected delivery outcomes and measurable benefits. None of these are known or have been shared with civil society, investors, the DVS providers or the public.

It must also benchmark how the same outcomes could be achieved with DVS Trust Framework alternatives, using objective measures such as cost-effectiveness, security performance, delivery timelines, accessibility, and user satisfaction.

Finally, the consultation must result in a consistent approach to digital credentials and personal data sharing across the economy resolving inconsistencies such as at Companies House. Here government communications have strongly promoted GOV.UK One Login and the Authorised Corporate Service Provider (ACSP) model, with no reference to the DVS sector. A basic online search shows ACSPs offering digital identity checks without DVS accreditation, raising concerns about regulatory inconsistency and ongoing fraud risk.

The consultation provides the opportunity to test and resolve these different perspectives and inconsistences against public opinion. It could provide transparency, restore confidence, demonstrate sound stewardship of public funds, and avoid unnecessary duplication.

It could be used to leverage and reinforce the UK's position as a global leader in trusted digital services while also advancing significantly the rights of citizens within the digital economy.

Strengthening trust through clear governance

The consultation should consider the need for independent oversight and stewardship of the personal data ecosystem to provide long-term stability and confidence through:

- long-term roadmap ownership
- impact assessment transparency
- coordination across related initiatives
- conflict-of-interest management

Such oversight would provide certainty to the DVS sector, relying parties, and government, for long-term investment independent of the priorities of any single administration where government acts as policymaker, regulator and delivery provider.

In effect, this would provide the equivalent of a Bank of England–style role for the governance and stewardship of personal data by:

- setting standards and governance
- ensuring national security, fraud resilience and public accountability
- maintaining trust lists, assurance requirements and regulatory oversight

The scope of such a body could also encompass related and complementary initiatives such as SMART Data within the Department for Business and Trade, Open Data Initiative research, university research within the Security, Privacy, Identity, Trust, Engagement Network (Sprite+), regulatory testing within the ICO Sandbox and EIDAS/International alignment, electronic signatures and electronic archiving. It is particularly important this body takes on the long-term public trust and education needed to cultivated adoption, resilience, and legitimacy over time.

Beyond strategic leadership, an independent authority would also manage real and perceived market risk concerning restrictions on credential distribution, storage, and avoidance of structural failure through monopolistic positions, unfair competitive advantage and exposure to foreign intervention. Specific concerns include:

- portability of credentials between accredited providers
- non-discriminatory acceptance across public services
- open interoperability based on published technical standards
- transparent cost benchmarking and objective performance measures
- providing a universal and inclusive service across all sections of the economy
- sunset measures when a particular DVS Provider ceases to trade or loses accreditation

Portability is particularly important for public trust. Citizens should not feel locked into a single provider or delivery route. Where credentials are issued, individuals should have the ability to move them between accredited wallets, and to access and manage their own information in a clear and user-friendly way.

While this consultation may resolve immediate issues, without independent oversight the certainty required for long-term investment and stable market development will remain absent.

Right to Work

The recent decision to reverse mandatory Digital ID for Right to Work (RTW) is welcome.

Given that combating illegal working, modern slavery, and organised crime were central drivers behind the original proposal, the private sector is well positioned to deliver comparable outcomes more quickly and at lower cost.

If government were to require employers to conduct digital RTW checks to obtain a statutory excuse against employing illegal workers, individuals could retain the choice over how they evidence their right to work, as they do today. They could continue to present physical documents or, if they wished, use digital credentials.

Those digital credentials could be issued either by government or by certified DVS providers, based on remote checks or employer-led physical verification of government-issued documents. This preserves existing RTW principles while enabling secure, reusable digital evidence.

Using DVS providers in this way would allow government to meet its objectives faster and more cheaply than developing a state-run system. It would also simplify compliance by enabling a consistent and simplified approach across both remote and face-to-face RTW checks.

Importantly, the model remains proportionate. The offence continues to be the employment of illegal workers, not the use of a specific technology. Employers, particularly SMEs, can continue to take a risk-based approach where right to work is already known. Where it is uncertain, use of a certified DVS provider provides a clear statutory excuse and recognised assurance.

Within this framework, the private sector could deliver at pace across several areas:

- **Getting people back to work through faster hiring by:**
    - issuing reusable RTW credentials by certified IDSPs for UK nationals where a medium level of assurance has been achieved (noting current regulation limits private RTW checks to 90 days);
    - extending the Home Office vouching policy to employers and building on vouching initiatives pioneered leading IDSPs; and
    - creating worker and volunteer wallets now emerging across the DVS sector.
- **Improving fraud and impersonation prevention:** The Home Office working with the private sector to develop a fraud signal solution that support threat assessment and operational decision this whilst satisfying the requirements of the DIATF and GPG45.
- **Supporting SMEs and the third sector** by encouraging proportionate and commercially viable compliance services to this group combined with tax deductible incentives to SMEs and local issued grants to the third sector.
- **Delivering place-based partnerships**, helping individuals move from hardship into volunteering, employment, and skills development.

Taken together, this approach allows government to meet its objectives while preserving choice and accelerating delivery through collaboration rather than compulsion. Such collaboration could accelerate delivery for RTW and digital ID more generally, reduce cost, support SMEs and the third sector, and improve fraud detection through structured signal-sharing.

A Proposal for Practical Partnership

Fraud, including identity misuse and impersonation, has become one of the defining pressures on the digital economy, steadily eroding public trust. It distorts markets and drives rising costs for citizens, businesses, and government alike. These challenges cannot be solved by government alone. Addressing them effectively requires constructive partnership between government, civil society, and the private sector, working through the DVS Trust Framework established by government.

There has been a perception in parts of government that the private sector lacks either the capacity or the appetite to meet the scale of digital transformation the government wishes to achieve. We would strongly challenge that view.

While policy uncertainty in the past year has slowed investment and driven early market consolidation, Association of Digital Verification Professionals continue to deliver at scale:

- approximately 5 million Right to Work checks each year;
- more than 2 billion identity and age checks globally, representing a major British export;
- around 11,000 skilled jobs sustained across the sector; and
- over £500 million in inbound investment, with further growth anticipated.

The UK's DVS sector is internationally competitive and strategically important, and one that government should actively champion and encourage. Political leadership is particularly needed now to drive adoption and reinforce a simple principle: data must move out of organisational silos and back into the hands of the people who own it.

The emphasis should be on choice. Enabling citizens to safely reuse verified information under their control, while giving businesses and public bodies the confidence to accept it — unlocking opportunity, protecting privacy, and supporting economic growth.

While government must issue digital credentials and modernise public services, the consultation should also strengthen the sector while enabling government to meet its objectives efficiently and inclusively.

To achieve this, the ADVP believes outcomes are best delivered when government sets the rules and markets innovate — particularly in a fast-moving, data-driven sector that underpins everything – including the use of AI. Citizens deserve meaningful control over who accesses their data, when, and for what purpose. That is what the DVS sector is designed to provide.

To ensure success, five conditions are critical:

1. Clear and stable policy direction
2. Defined roles for government and the market
3. Independent oversight, certification and transparent governance
4. Continued commitment to inclusion, privacy, trust and user choice
5. Practical decisions based on outcomes, speed, national security and cost-effectiveness

ADVP stands ready to engage constructively as the consultation is prepared and to contribute fully once it is published.