



Office for Digital
Identities & Attributes



Department for
Science, Innovation
& Technology

Digital Verification Services

2026 Annual Report on the operation of Part 2 of Data (Use and Access) Act 2025

Published 14 July 2026

Contents

Contents	1
Foreword by the Minister for Digital Government and Data.....	2
Executive summary	4
Operation of measures carried out under Part 2 of the Data (Use and Access) Act 2025.....	6
1. The UK DVS trust framework and supplementary codes	7
2. DVS register.....	11
3. Information sharing power.....	15
4. Financial and resource information	17
5. Trust mark.....	18
Report on additional activities carried out by the UK Office for Digital Identities and Attributes to complement statutory duties	20
6. Consumer and market outcomes	21
7. International policy and engagement.....	24
8. Roadmap of OfDIA's expected activity in the year ahead.....	25

Foreword by the Minister for Digital Government and Data

Trusted digital verification services (DVS) are vital to the success of the modern digital economy. As more of our everyday interactions move online, people must be able to prove things about themselves securely, simply and with confidence. Businesses and public authorities need to know which digital checks they can really trust.

Last summer, this government passed the Data (Use and Access) Act 2025. This set out a clear ambition: to make the UK a world leader in facilitating the use of trusted DVS across the economy and to give people a secure and privacy-preserving way to prove things about themselves online. This first annual report marks an important milestone in delivering that ambition.

This annual report shows a growing number of DVS and providers are certified against the UK's statutory trust framework and listed on the DVS register. This demonstrates momentum from a market that is generating more than £2 billion in revenue and contributing more than £800 million to the UK economy and shows that industry is responding to the clarity and certainty the Act was designed to provide.

But we cannot be complacent. Trust is not built by legislation alone. People need to know that DVS are safe, inclusive and designed with their interests at heart. This means businesses, public authorities and providers working together to make DVS easier to understand, easier to use and easier to trust.

This is why the UK Office for Digital Identities and Attributes (OfDIA), in the Department for Science, Innovation and Technology, is working with colleagues across government to unlock real world use cases, such as supporting the use of registered DVS under the Money Laundering Regulations and for proof of age in the sale of alcohol.

Looking ahead, OfDIA will continue to support adoption of DVS across more key sectors of the economy. On behalf of the Secretary of State for Science, Innovation and Technology, OfDIA will work to ensure the DVS regime keeps pace with technology and market developments. OfDIA will continue to work closely with the Government Digital Service as they develop GOV.UK One Login and the GOV.UK Wallet, improving how people access public services in a way that is secure, simple and user-centred. OfDIA will support efforts to introduce the national digital ID by ensuring that the principles and standards of the DVS trust framework are baked into the development of the scheme. OfDIA will also continue to work with international partners and standards bodies.

All these activities will support a shift towards a more modern, efficient and inclusive digital economy where trusted DVS make everyday transactions easier, strengthen

protections against fraud, and give people more control over how their information is shared. That's the future I want to see for the UK.

The Rt Hon Ian Murray MP

Minister for Digital Government and Data



Executive summary

Pursuant to section 53 of the Data (Use and Access) Act 2025 (the Act), the Secretary of State is required to prepare and publish annual reports on the operation of the provisions in Part 2 of the Act, including their commencement progress and how they are operating in practice.

This annual report sets out the government's progress in establishing and maintaining the UK's statutory regime for DVS providers who choose to be certified against government rules. Specifically, to fulfil the Secretary of State's statutory duty under section 53 of the Act, chapters 1 to 5 of this report provide an account of the operation of the relevant measures under Part 2 of the Act, including the DVS trust framework and supplementary codes (sections 28 to 31), the DVS register (sections 32 to 44), the information sharing power referred to as 'information gateway' (sections 45 to 49) and the UK CertifID trust mark (section 50).

The annual report also includes some non-statutory and wider contextual information to support understanding of the environment in which the Part 2 statutory regime is operating. This information is covered in chapters 6, 7 and 8 of this report. Chapters 6 and 7 cover consumer and market outcomes and international policy and engagement, while chapter 8 sets out a roadmap for the expected direction of travel for the wider DVS regime over the next reporting period.

During this reporting period, the Office for Digital Identities and Attributes (OfDIA) has moved from legislative design to practical implementation of the Act and continued to support market development. As of July 2026, the DVS register lists 46 providers offering 64 certified services across identity, attribute, orchestration, holder and component service roles. Many of these services are also certified against supplementary codes for right to work, right to rent and Disclosure and Barring Service checks.

Readers should note that independent certification plays an important role in the DVS ecosystem in the UK alongside the statutory regime under Part 2 of the Act. Certification by independent conformity assessment bodies (CABs) accredited by United Kingdom Accreditation Service provides assurance that services on the DVS register are being provided in compliance with the DVS trust framework and any relevant supplementary codes.

This report also helps the government identify where the operation of the trust ecosystem underpinned by the Act can continue to improve, including on data standards, vouching, inclusion and accessibility, and the way identities are checked digitally and linked to the right person. These findings support the priorities set out later in this report and will help strengthen trust, consistency and inclusion across the DVS ecosystem in the UK.

A key milestone was the publication of version 1.0 of the UK DVS trust framework and supplementary codes. This reflects several years of development, consultation and testing, and strengthens requirements on governance, privacy, security, inclusion, accessibility, technical specifications and user experience.

This report also sets out the government's progress on the implementation of the information sharing power under section 45 of the Act, which will allow public authorities to disclose information about an individual to registered DVS providers where that individual has requested the services of the particular DVS, that particular service is registered on the DVS register, and the DVS needs the information being requested to deliver those services. OfDIA has drafted the statutory Code of Practice about the disclosure of information under section 45 and engaged with devolved governments, the Information Commissioner's Office (ICO), other government departments, the industry and civil society. Subject to Parliamentary approval, government intends to commence the information sharing power under section 45 in the next reporting period.

The wider market continues to show economic value and user demand. The 2026 Digital Identity Sectoral Analysis, which was published on GOV.UK on 8 July 2026 , identified 275 firms providing digital identity products and services in the UK, generating an estimated £2.027 billion in annual revenue and supporting 9,624 full-time equivalent roles. It also found that 77% of UK consumers had previously used digital identity services.

Looking ahead, the next phase will focus on scaling adoption and strengthening the regime. Priorities include supporting certification against version 1.0 of the DVS trust framework, issuing the UK CertifID trust mark for use by registered DVS providers, developing a machine-readable DVS register, implementing the information sharing power under section 45 of the Act, encouraging and supporting more CABs to participate in the market and consulting on future updates to the DVS trust framework. These priorities are set out in chapter 8 at the end of this report, which explains the expected direction of travel for the DVS regime over the next reporting period.

Together, these developments mark a significant step in establishing a trusted, inclusive and secure DVS ecosystem for the UK.

Operation of measures carried out under Part 2 of the Data (Use and Access) Act 2025

1. The UK DVS trust framework and supplementary codes

Legislative context

Section 28 of the Act requires the Secretary of State to prepare and publish the DVS trust framework, while section 29 of the Act requires the Secretary of State to prepare and publish one or more sets of rules concerning the provision of DVS which supplement the DVS trust framework and which are referred to as supplementary code(s). Sections 28 to 31 set out the duties imposed and powers conferred on the Secretary of State in respect of the DVS trust framework and supplementary codes, including her duty to consult the Information Commissioner and other appropriate stakeholders on its rules, and her duty to carry out at least one review every twelve months of the DVS trust framework and any active supplementary codes.

Development and consultation

Since 2021, the DVS trust framework has evolved through alpha (0.1 and 0.2), beta (0.3), non-statutory gamma (0.4) and statutory gamma (0.4) which was the first statutory trust framework under section 28 of the Act on 1 December 2025. Each iteration involved extensive consultation with industry and regulators and alignment with international standards. The latest version of the DVS trust framework is version 1.0¹, which was published on 9 June 2026. Version 1.0 will come into effect on 1 September 2026, subject to successful accreditation of conformity assessment bodies by the UK Accreditation Service (UKAS).

The DVS trust framework

The DVS trust framework sets out the rules that organisations must meet to provide certified DVS in the UK. It covers organisational governance, information security, privacy and data protection, technical specifications and user experience. It emphasises the importance of inclusive design, requiring services to follow web accessibility standards, encouraging the acceptance of a wide range of evidence types (e.g. vouching), and requiring organisations with certified services to submit annual inclusion monitoring reports.

The DVS trust framework was renamed from its former title, the 'UK digital identity and attributes trust framework', to the 'UK digital verification services trust framework' to better align with the terminology set out in section 28 of the Act.

Supplementary codes

Supplementary codes for digital right to work, right to rent and Disclosure and Barring Service (DBS) checks set rules which build on the DVS trust framework to

¹ [UK digital verification services trust framework \(1.0\)](#)

help DVS providers certified against them show that their services meet government requirements in those use cases. Upon the commencement of section 29 of the Act on 1 December 2025, OfDIA has published 1.0 versions of each supplementary code alongside the 1.0 version of the DVS trust framework, making it clearer what code-certified DVS must share with relying parties when they share a right to work, rent or DBS check output. To be certified against a supplementary code, a service must also be certified against the corresponding version of the DVS trust framework.

During this reporting period, section 30 was commenced on 1 December 2025, and the power under section 30 has not been exercised.

Review and updates

Section 31 requires that the DVS trust framework and any active supplementary codes be reviewed at least every 12 months. The 1.0 version of the DVS trust framework marks the first revision since the passing of the Act. In producing the 1.0 DVS trust framework, OfDIA consulted with the ICO as required under the Act, and with other appropriate stakeholders, including certified DVS providers.

Key changes following the 1.0 version of the DVS trust framework include:

- Providers certified and registered against the 1.0 version will, for the first time, be able to use the *UK CertifID* trust mark. The 1.0 version sets rules governing trust mark usage. New versions of all the supporting documents (additional guidance documents setting out the standards for particular roles or processes) were published alongside the 1.0 version of the trust framework.
- The 1.0 version of the trust framework also includes the first dedicated rules for orchestration services, such as ‘hub’ services that allow relying parties to work with others, and new rules for holder services. Holder services, such as wallets, are services requested by an individual that use information from a third party to verify a fact about that individual and then confirm that verified fact to another person. These rules will help relying parties understand the identities and attributes they hold.
- More broadly, various documents cited in the 1.0 version of the trust framework have also been updated. This includes the data schema, which sets out a machine-readable way to describe identity checking and account authentication outcomes, and rewritten vouching guidance, which will support inclusion by enabling vouches to be used as part of identity checking.

Looking ahead

After iterative development over five years, drawing on the outcome of consultation and engagement with a wide range of stakeholders, the DVS trust framework is now a mature set of rules which provides an essential basis for certified and registered DVS to operate in the market.

OfDIA's plan is to ensure that the DVS trust framework and supplementary codes keep pace with innovation in the sector by accommodating new technologies, delivery models and service types. This includes supporting effective certification, enabling programmatic checking capabilities through the DVS register, and helping to drive wider adoption across the economy as new use cases emerge, such as the use of registered DVS for alcohol purchases. OfDIA will also continue to ensure that the DVS trust framework supports appropriate protections for individuals and businesses as security and fraud risks evolve.

Programmatic checking of DVS

To make the most of sector innovation, OfDIA is now exploring whether further rules are needed to enable services which support relying parties to programmatically check the digital identities and attributes presented to them. OfDIA is looking to services that are already doing this, and existing international standards work in this space, to understand what good programmatic checking looks like.

Adoption of DVS in more use cases

To enable adoption of registered DVS in the alcohol-purchasing use case and look toward further use cases that require age verification, OfDIA is exploring whether to publish new rules on trustworthy digital age verification checks. OfDIA is considering whether such rules would be best contained in a dedicated supplementary code for digital age verification. As part of this, OfDIA is planning to explore options for enabling children to prove their age online in a safe and privacy preserving way. OfDIA will continue to support wider government work to enable the use of registered DVS for age verification and other high-value use cases in regulated sectors. This includes work with the Home Office on enabling registered DVS to be used for age verification in the sale and supply of alcohol, alongside broader work to consider how trusted DVS could support other age-restricted products and services.

Protecting individuals and businesses from emerging security threats

To ensure the right protections are in place for emerging security threats, OfDIA is also reviewing the security and fraud sections of the DVS trust framework and exploring how to improve the supporting authentication guidance by adopting existing best practices in the digital identity sector and beyond.

Promoting inclusion in DVS

OfDIA is committed to inclusion; everyone that wants to use digital identity should be able to. After addressing the priorities already outlined above, OfDIA will look further into how the identity checking guidance, and the vouching guidance which sits alongside it, can be further improved to help ensure anyone who wants to use DVS can do so.

Collaborative development of the DVS trust framework

OfDIA cannot do this work without working closely with expert stakeholders. To build on OfDIA's longstanding open policymaking approach, it is planning to publish a working draft of the DVS trust framework and its supporting documents on GitHub before finalising their next version. This will enable stakeholders to propose specific changes to the content of the trust framework and its supporting documents. It will also allow stakeholders to more easily see how these documents develop between draft and final versions. OfDIA will consider suggestions made through this process, as part of its wider activities to fulfil the relevant consultation requirements in the Act. The final and official versions of these documents will be published on GOV.UK.

2. DVS register

Legislative context

Section 32 of the Act requires the Secretary of State to establish and maintain a publicly available register of providers offering DVS and certified against the DVS trust framework, referred to as the DVS register. Sections 33 to 44 set out a range of functions that help to support the effective operation of the DVS register.

Sections 40, 42, 43 and 44 place a duty on the Secretary of State to remove information from the DVS register when specific circumstances apply. These circumstances include when a provider asks for information to be removed, the provider ceases to provide all of their registered services and where they no longer hold a certificate from an accredited CAB certifying that at least one of those services is provided in accordance with the DVS trust framework or the supplementary code to which the service was certified against.

Sections 34 and 41 set out the Secretary of State's powers to refuse an application or remove a provider from the DVS register in specific circumstances. These circumstances include where refusal or removal is necessary in the interests of national security, and where the Secretary of State is satisfied that a DVS provider is not in compliance with the DVS trust framework or a supplementary code. Section 41 also allows the Secretary of State to remove a provider from the register for failing to provide information in accordance with an information notice under section 51. The powers in sections 34 and 41 may only be used after giving notice and allowing representations from the provider in question.

Together, these functions create an authoritative and up to date record of DVS providers and services registered with OfDIA that can be relied upon by a range of stakeholders.

Operation

Sections 32 to 44 were commenced on 1 December 2025.

The DVS register² is a public list of registered DVS established and maintained by OfDIA acting on behalf of the Secretary of State. OfDIA first published the non-statutory DVS register on GOV.UK in March 2025, which was then replaced by the statutory DVS register upon commencement of section 32.

To be listed on the DVS register, providers must be certified against the trust framework by an accredited CAB and have made an application to OfDIA to join the register which complies with the determination made under section 38. OfDIA must

² [Find registered digital identity and attribute services](#)

also have concluded that neither of the grounds for refusal to register as set out in section 34 applies. Providers must also pay any applicable fee where required.

OfDIA is responsible for maintaining the DVS register, including the processing of applications to join the register. CABs must notify OfDIA if a provider's certificate is suspended or withdrawn so that the service is removed from the register. Services will be automatically removed from the register if their certificate expires.

The DVS register displays information about each registered provider's service, including the service name, provider name, role types, supplementary codes, and certificate issuance and expiry dates. The register allows filtering by role type and supplementary codes and provides both certification details and company information.

Compliance and monitoring

When processing applications OfDIA performs a range of public interest checks to establish a provider's compliance with the DVS trust framework and to determine their eligibility to join the register. The type of checks performed are derived from the Act itself, the DVS trust framework and the certification scheme. These checks provide the basis on which we may refuse an application or remove a provider from the register.

OfDIA also performs the same checks on a regular basis after a provider has joined as part of its monitoring. This monitoring helps ensure providers remain in compliance with the DVS trust framework and remain eligible to be on the register.

The type of checks OfDIA performs include, but are not limited to, checking a provider's ownership chain for national security risks, whether they are involved in any outstanding proceedings such as patent disputes, have any prior convictions for corruption, bribery or money laundering, and directors' checks. OfDIA also assesses a provider's marketing materials to ensure they are not misrepresenting or making misleading claims about themselves to market or bringing the DVS trust framework into disrepute.

OfDIA applies these checks to protect the integrity of the register and performs them in a proportionate and consistent manner to ensure providers are treated fairly. If OfDIA identifies any issue during our checks, OfDIA typically engages with the provider and/or the CAB to take remedial action or ask for further information to be provided. However, the action OfDIA takes can vary on a case-by-case basis depending on the nature of the issue; OfDIA retains the power to refuse to register service providers or to remove service providers from the register if appropriate.

Activity summary

OfDIA has performed public interest checks on every registered provider and service at least once since being registered, with most providers and services having been checked at least twice within this reporting period. Performing these checks allows OfDIA to consider the factors relevant for deciding whether the Secretary of State should exercise the powers under sections 34 and 41 (i.e. the power to refuse registration in the DVS register, and the power to remove a provider from the DVS register). During this reporting period, the powers under sections 34 and 41 have not been exercised.

On 1 April 2026, five DVS providers no longer held any certificate from an accredited CAB following the expiry of their certificate issued against the beta (0.3) version of the DVS trust framework. They were removed from the DVS register in line with the Secretary of State's duty under section 42(1)(c). Apart from this, the Secretary of State has not exercised her duty to remove information from the DVS register under sections 40, 42, 43 and 44.

Looking ahead

Over the course of the next reporting period, OfDIA will continue to make improvements to the DVS register. These will include giving registered DVS providers an easier way to manage their registration, make change requests to their information on the register, and access their unique trust mark.

OfDIA is also developing a machine-readable layer to supplement the current service and enable programmatic checking against the DVS register. This will enable registered DVS providers, relying parties and public authorities where relevant, to use cryptographically secure means to check the services they are interacting with are on the DVS register.

This will support further use of DVS at scale in transactions across the economy. This will be particularly helpful where certification against the DVS trust framework and registration in the DVS register is a regulatory or contractual requirement. For example, in the use of registered DVS to carry out age-verification checks to purchase alcohol when those have been enabled through secondary legislation, the service(s) involved in the transaction will be able to automatically and securely demonstrate their certification at the point of sale.

Similarly, the machine-readable layer is expected to underpin the use of the information sharing power in section 45 of the Act (covered in detail in the next section). Registered DVS providers making requests for information on behalf of individuals under that section will need to demonstrate to the disclosing public authority they are on the DVS register, and OfDIA envisages the machine-readable layer to facilitate this securely, programmatically, and at scale.

This service is in development with a planned launch date of Winter 2026.

3. Information sharing power

Legislative context

Section 45 of the Act allows public authorities to disclose information about an individual to registered DVS providers where that individual has requested the services of the particular DVS, that particular service is registered on the DVS register, and the DVS needs the information being requested to deliver those services. This is also referred to as the “information sharing power”.

Sections 46 to 48 of the Act relate to His Majesty’s Revenue and Customs (HMRC), the Welsh Revenue Authority and Revenue Scotland respectively. These provisions provide additional safeguards for any information disclosed by these bodies through the information sharing power under section 45.

Section 49 of the Act requires the Secretary of State to prepare and publish a Code of Practice, to which public authorities must have regard in disclosing information under section 45. The Code provides guidance for those public authorities disclosing information to support consistent and appropriate implementation of the power.

The Code must be laid before Parliament and approved by both Houses before publication. The Code will be published before section 45 is commenced.

Operation

During this reporting period, section 49 was commenced, and OfDIA has been preparing for the commencement of section 45. OfDIA has drafted the Code and consulted on the Code with the devolved governments, the ICO, multiple government departments and several other stakeholders in industry and civil society, as required by section 49 of the Act.

As His Majesty’s Revenue and Customs (HMRC), the Welsh Revenue Authority, and Revenue Scotland are working on their preparedness for exercising their information sharing power under section 45, sections 46 to 48 have not been commenced, and section 45 is not being prepared for commencement in respect of these three public authorities during this reporting period.

Looking ahead

OfDIA plans to finalise the draft Code and lay it before Parliament for approval, with the aim of it being published by the end of 2026. Once the Code has been approved, section 45 will be commenced.

All UK public authorities are in scope, but as outlined above, the power will not initially be in force with regards to HMRC, Revenue Scotland and the Welsh Revenue Authority.

Section 45 will be commenced for these public authorities later (along with sections 46, 47 and 48). OfDIA will work closely with these public authorities to establish a timeline for commencement as soon as is practicable.

To prepare for commencement, OfDIA intends to publish information on GOV.UK and on its *Enabling digital identity* blog for public authorities and registered DVS providers. This content will be developed in collaboration with public authorities and DVS providers to help establish and improve processes and share best practice. OfDIA has already published a blog post³ explaining the information sharing power and how it could operate in practice. OfDIA is engaging with several government departments to understand organisational readiness and how OfDIA can best support public authorities to make use of this power.

³ [The information gateway: enabling secure sharing of information held by public authorities with trusted digital verification services](#)

4. Financial and resource information

Operation

During this reporting period, OfDIA focused on delivering and operating the statutory regime set out in Part 2 of the Act. This included establishing and maintaining the DVS trust framework, supporting certification and accreditation processes which sits alongside Part 2, operating the DVS register, and preparing for the introduction of the information sharing power.

OfDIA delivered these functions as part of the Department for Science, Innovation and Technology's Spending Review 2025 settlement. In 2025/26, OfDIA had operating costs of £5,690,783. That includes all staff costs, non-pay spend, and capital expenditure on the DVS register.

Fees

Section 39 of the Act gives Secretary of State the power to introduce fees in connection with applications for registration and ongoing inclusion on the DVS register. During this reporting period, OfDIA has not implemented fee regulations and did not charge fees to providers.

Looking ahead

At this stage, OfDIA does not plan to introduce fees for joining or remaining on the DVS register. Over the next reporting period OfDIA will undertake further policy work to consider the approach to fees including assessing potential approaches to fee setting, considerations of cost recovery, market impact and proportionality.

Knowing that any decisions on fees will require a carefully considered and transparent approach, OfDIA will continue to engage with stakeholders and will provide further updates and will be inviting views from stakeholders to help inform OfDIA's approach.

5. Trust mark

Legislative context

Section 50 of the Act gives the Secretary of State the power to designate a trust mark for use by registered DVS providers. OfDIA is responsible for issuing and managing the use of the trust mark. This statutory basis ensures that the trust mark is not only a visual indicator of a service's registered status, but a formally governed assurance mechanism, giving individuals, businesses and public sector organisations confidence that a service has been assessed as meeting consistent, government-backed standards for security, reliability and trustworthiness.

Operation

Section 50 was commenced on 1 December 2025. OfDIA, acting on behalf of the Secretary of State, designated the trust mark, UK CertifID, in March 2026 and provided more details about the trust mark in the 16 March 2026 blog post⁴.

Version 1.0 of the UK digital verification services trust framework which was published on 9 June 2026 includes rules on the use of the UK CertifID trust mark, explaining when and how it should be used by certified and registered providers to help users and relying parties identify services that meet the government rules.

Looking ahead

Once registered DVS providers have obtained certification against version 1.0 of the DVS trust framework and are listed on the DVS register, they will be issued with a trust mark for their use under licence. The trust mark will only be available for use by services that have successfully achieved certification against 1.0 (and subsequent versions) and are listed on the DVS register.

The use of the trust mark is intended to balance accessibility for providers with robust assurance for users and is underpinned by two complementary components developed by OfDIA: section 14 of the DVS trust framework defines the eligibility and conditions for its use, and a coordinated approach to monitoring and enforcement that aims to protect the integrity of the trust mark over time.

The policy framework provides a structured and transparent approach to enabling providers to use the trust mark. It sets out clear eligibility requirements, including the need for valid certification and registration, alongside formal Terms of Use that are embedded within the certification and registration process.

⁴ [UK CertifID: a mark of trust in digital verification services](#)

Supporting guidance and usage materials translate these requirements into practical application, ensuring consistency in how the mark is displayed while reinforcing its role as a trusted signal of compliance. This approach will enable providers to adopt the trust mark with confidence, while maintaining a consistent and recognisable standard across the market.

To sustain confidence in the trust mark, OfDIA will undertake ongoing monitoring of how the trust mark is used in practice. This will include verifying continued eligibility through the register, reviewing usage across digital channels, reviewing use against the Terms of Use and maintaining records of authorised users.

Where non-compliance is identified, the Secretary of State will decide on the proportionate enforcement action to be taken, ranging from requesting removal of the trust mark to more serious escalations in cases of persistent or significant misuse. This oversight ensures that use of the trust mark is limited to certified and registered providers and that the credibility of the scheme is actively protected.

The trust mark is expected to play an increasingly important role in supporting the growth and maturity of the UK digital verification ecosystem.

Before that OfDIA will also publish the Terms of Use for the trust mark on GOV.UK so that providers and users of DVS understand the framework in which it can be used. OfDIA will also start carrying out trust mark monitoring activities to ensure it is being used in a legally compliant way.

**Report on additional activities carried out by the UK Office
for Digital Identities and Attributes to complement
statutory duties**

6. Consumer and market outcomes

Sector analysis

OfDIA commissions an annual analysis of the UK digital identity sector to understand any trends in the market and monitor its performance. The 2026 edition of the Digital Identity Sectoral Analysis covering activity in 2025, was published on 8 July 2026 , and found that:

- **275 firms** are currently providing digital identity related products and services in the UK.
- The sector generated an estimated **£2,027 million in annual revenue** in 2024/2025.
- Estimated **Gross Value Added (GVA)** reached **£1,037 million**.
- **GVA per employee is £107,800**, approximately 46% above the estimated UK workforce average.
- An estimated **9,624 Full-Time Equivalents (FTEs)** are employed in digital identity roles across the UK.
- **75% of providers** are involved in identity or attribute verification, with document-based verification (60%) and biometrics and liveness detection (57%) the most common sub-categories. Providers are broadening their offerings: professional and credential verification rose from 28% to 55%, and age assurance from 23% to 31%.
- The sector is **highly internationalised**. 73% of firms are UK-headquartered, of which 36% have at least one international office. Over a third of the sector's c.£2bn revenue (£686m) is attributable to export activity.
- **Investment activity** totalled £49 million across 14 deals in 2025. Approximately three in ten dedicated firms have received external investment since incorporation. Merger and Acquisition (M&A) activity has continued, including the acquisitions of TrustID, Keyless, and DataTools.

These figures are similar to the 2025 results, indicating market conditions have not changed significantly between 2023/24 and 2024/25. The full report is available on GOV.UK⁵.

⁵ [Digital Identity Sectoral Analysis Report 2026](#)

Adoption

With 64 services from 46 providers on the register, the DVS ecosystem is reaching more people. The 2026 sectoral analysis found:

- There are almost 4,700 unique businesses, organisations and partnerships across providers,
- Providers increasingly frame their value proposition around **compliance and user experience** rather than purely operational efficiencies,
- 77% of UK consumers used digital identity services, rising to 85% among adults under 45 years old.

Among those who do not use digital identity services (23%), the most commonly cited reasons were **preference for physical ID (29%)** and not having had to prove their identity (29%).

Inclusion

The government is committed to ensuring that DVS are inclusive and accessible for anyone who chooses to use them. To support our understanding of the issues associated with inclusion and accessibility, all DVS providers are required to submit an inclusion monitoring report at least annually. Key findings from the 2025 Inclusion Monitoring Report⁶ include:

- 60% of organisations surveyed adhere to the Web Content Accessibility Guidelines 2.0 medium conformance or higher, up from 54% in 2024.
- 55% of organisations surveyed report that they collect demographic data about their users. Of these services, 42% are using this data to monitor the inclusivity of their service.
- 47% of organisations surveyed report that they offer non-digital routes for users to access support (telephone or in-person). Of those that don't, the survey identified that the organisation who has contracted out their digital identity services out to a registered DVS provider often provides the support mechanisms for consumers themselves (rather than expecting the DVS to do this for them).
- 73% of organisations surveyed offer at least one accessibility feature, such as text magnification or compatibility with assistive technologies, up from 65% in 2024.

In their inclusion monitoring returns in 2025, DVS providers cited various challenges to improving inclusive practice, most notably cost and lack of access to government-held data for alternative authoritative sources of information for those individuals who do not have a driving licence or passport.

⁶ [Inclusion Monitoring Report Findings](#)

These findings underline the importance of continuing to strengthen the evidence base on inclusion and ensuring that all certified providers consider accessibility and user experience as part of their service design.

Looking ahead, OfDIA is currently preparing to publish the 2026 Inclusion Monitoring Report that will provide further insight and evidence on the inclusivity of the certified and registered DVS market. The report will inform OfDIA's approach to encouraging the market to grow in a way which supports inclusion. Key challenges include improving inclusion for people without traditional identity documents and ensuring fair access to government data. OfDIA will explore options with stakeholders to address these challenges.

Complaints and incidents

OfDIA oversees complaints relating to services certified under the DVS trust framework. This includes managing complaints on the conduct of registered providers, working with relevant bodies where issues fall within their remit, and supporting appropriate escalation or redress mechanisms where required.

In line with the DVS trust framework, DVS providers are required to maintain appropriate records of complaints in accordance with their information management policies and to make this information available to OfDIA on request.

7. International policy and engagement

OfDIA is taking a number of steps to lay the foundations for secure and trusted use of digital identities, credentials and verification services across international borders.

Evidence gathering

In February 2026, OfDIA published the results of a survey on the international use of digital identities and credentials⁷. Of the providers who responded, 79% identified regulatory diversity and disparate technical standards as major barriers to cross border use, 79% wanted government involvement to help remove barriers to interoperability and 62% supported mutual recognition of national trust frameworks.

OfDIA will continue to gather evidence on the barriers and opportunities for international use of digital identities and credentials. This will include further engagement with industry, international partners and standards bodies to build the government's understanding of priority use cases, interoperability challenges and the role that different services under the DVS trust framework could play in supporting trusted cross-border use of digital identities and credentials.

International engagement and standards development

OfDIA plays an active role in international standards development through strategic engagement with organisations such as the British Standards Institute (BSI), the International Organisation for Standardisation (ISO) and the International Telecommunications Union (ITU). Active engagement in international standards development is strategically important as it enables us to influence global standards in line with our policy priorities while at the same time supporting the cross-border interoperability of trusted digital identity systems and frameworks.

You can find out more about our international standards work in this blog post⁸, published in April 2026.

OfDIA also participates in global conferences and events. Over the last year, these have included the EU Digital Identity Launchpad (December 2025), the European Identity and Cloud Conference (May 2026) and Identity Week Europe (June 2026).

⁷ [International Use of Digital Identities and Credentials: Stakeholder survey responses](#)

⁸ [Why international standards matter for digital identity in the UK](#)

8. Roadmap of OfDIA's expected activity in the year ahead

The roadmap below sets out the expected areas of activity for OfDIA over the next reporting period. It reflects the OfDIA's current priorities for strengthening the DVS ecosystem, which are to support adoption across the economy, improve the certification and registration processes for DVS providers, and ensure that the DVS regime remains secure, inclusive and responsive to emerging risks.

The roadmap is not underpinned by any statutory footing and is provided for information only. It should not be taken as an official commitment of future government priorities, which are subject to change.

Certification, registration and the trust mark

Over the next reporting period, DVS providers will be able to certify their services against version 1.0 of the DVS trust framework once it comes into force.

OfDIA will also begin issuing the UK CertifID trust mark to DVS providers whose services are certified and registered against version 1.0 of the DVS trust framework. The trust mark is expected to support confidence in the DVS ecosystem by helping individuals, businesses and public sector organisations identify services that have been certified and registered against government rules.

Into 2027, OfDIA will seek to strengthen the certification process, including by encouraging a greater range of accredited conformity assessment bodies with the necessary resources and expertise to certify DVS providers against the DVS trust framework.

Programmatic checking and the DVS Register

OfDIA will make publicly available a machine-readable layer of the DVS register to support programmatic checking capabilities. This will help registered DVS providers, relying parties and public authorities check, in a secure and scalable way, whether a service is listed on the DVS register and certified against the relevant rules.

This work is expected to support the use of registered DVS at scale across the economy, particularly where certification and registration form part of the relevant regulatory and/or contractual requirements for DVS to be used for digital checks. It will also support future use of the information sharing power under section 45 of the Act, where public authorities will need to confirm, among other things, that a DVS provider is registered before disclosing information to them.

Adoption and new use cases

OfDIA will continue to support work by other government departments to enable the use of registered DVS for high-value use cases in regulated sectors. This includes

work to support the use of registered DVS for the supply of age-restricted products and services.

OfDIA will also support government plans to prevent social media platforms from offering their services to under-16s, by exploring the role that trusted DVS providers could play in supporting highly effective age assurance checks.

Into 2027, OfDIA will investigate whether further supplementary codes could drive adoption in additional use cases or strengthen trust and consistency across the DVS ecosystem.

Trust framework review and future rules

OfDIA will begin engagement and consultation on the next version of the DVS trust framework as part of the annual review cycle. This will help ensure that the DVS trust framework and supplementary codes remain aligned with industry needs, emerging risks and technological developments.

Future work will consider whether further updates are needed to support new technologies, delivery models and service types, while maintaining appropriate protections for individuals and businesses.

OfDIA will also continue to consider whether further supplementary codes are needed to support adoption in additional use cases or to strengthen consistency across the DVS ecosystem.

Inclusion and user outcomes

OfDIA will publish the 2026 Inclusion Monitoring Report. This will provide further evidence on inclusion across the certified and registered DVS market and will inform OfDIA's approach to supporting the market to grow in a way that helps improve accessibility, inclusion and user confidence.

Information sharing power ('information gateway')

The statutory Code of Practice under section 49 of the Act about the disclosure of information under section 45 will be laid in Parliament.

Section 45 of the Act will be commenced once the Code of Practice has been approved by Parliament. Following commencement, the information sharing power will be available for public authorities to disclose information relating to individuals with registered DVS where the conditions in section 45 are met.

OfDIA will continue to support public authorities and registered DVS providers to prepare for the commencement of the information gateway power, in order to help ensure a consistent implementation of the power across the DVS ecosystem.

Wider regulatory and institutional development

OfDIA will continue to work with regulatory bodies in sectors covered by the Money Laundering Regulations to support consistent implementation of guidance on the use of digital identity services for customer due diligence. This will include helping to ensure that relevant guidance is reflected appropriately in sectoral guidance and implemented consistently by firms operating in those sectors.

OfDIA will also develop proposals for its permanent institutional home for governance, as committed to in the government's response to the 2021 consultation on digital identities and attributes. This work will support the long-term sustainability of the DVS regime and help ensure that OfDIA can continue to provide effective oversight, coordination and policy leadership as the DVS ecosystem develops.