

COMPLIANCE GUIDE

Government & Public Services Compliance in the United Kingdom

COUNTRY **United Kingdom**

INDUSTRY **Government & Public Services**

LAST UPDATED **16 October 2026**

KEY REGULATORS **Office for Digital Identities and Attributes · Home Office · Information Commission**

Key takeaways

- There is no licence to provide identity checks in the UK, but providers that want government recognition must be independently certified against the statutory trust framework and listed on a public register run for the Secretary of State.
 - From 1 October 2026, an employer that uses a digital provider for a right to work check must use one that is registered for right to work checks. An unregistered provider no longer protects the employer against a civil penalty of up to £60,000 per illegal worker.
 - Online and in-person identity checks are scored on the same scale, but the very highest scores for checking a document and matching a face can only be reached in person, under supervised conditions.
 - A national digital identity held in the GOV.UK Wallet is planned and will be voluntary. It is not yet law: the bill was announced in May 2026 and the government has not yet published its consultation response (as of October 2026).
 - Face matching uses special category data, so a provider normally needs explicit consent and must offer people a route that does not use their biometrics.
-

The UK market for public-sector and government-recognised identity checking is open to private providers. The government operates its own sign-in and identity service, GOV.UK One Login, and private providers serve regulated uses such as right to work, right to rent and criminal record checks through a certification and registration scheme set up by Part 2 of the Data (Use and Access) Act 2025.

The principal authorities are the Office for Digital Identities and Attributes (OfDIA), which runs the trust framework and the register; the Government Digital Service, which runs GOV.UK One Login; the Home Office, which sets the right to work and right to rent rules; and the Information Commission, which regulates data protection.

The biggest obstacle for a new entrant is certification: a provider cannot join the register without a certificate from an accredited conformity assessment body, and the framework is moving from version 0.4 to version 1.0 during 2026 to 2028.

CONTENTS

- 1 Who regulates this sector
- 2 Licensing and authorisation
- 3 Identity framework (AML rules do not apply)
- 4 Identity verification and onboarding
- 5 Digital channels: what's different
- 6 Data protection and biometrics
- 7 Sector-specific obligations
- 8 Risk indicators and red flags
- 9 Enforcement and penalties
- 10 Recent changes and what to watch
- 11 What this means for identity verification
 - Sources

1 Who regulates this sector

Identity rules for public services are set centrally and apply across the UK, with the exception of right to rent checks, which apply in England only. Policy responsibility is split between the bodies below.

Authority	Remit	Level	Official site
Office for Digital Identities and Attributes (OfDIA)	Trust framework, supplementary codes, certification scheme and the digital verification services (DVS) register, on behalf of the Secretary of State	UK-wide	gov.uk/ofdia
Government Digital Service	GOV.UK One Login, the GOV.UK One Login app and the GOV.UK Wallet	UK-wide	gov.uk/gds
Cabinet Office	National digital ID policy and the planned Digital Access to Services Bill	UK-wide	gov.uk/cabinet-office
Home Office (UK Visas and Immigration, Immigration Enforcement)	Right to work and right to rent checks, civil penalties	UK-wide (right to rent: England)	gov.uk/home-office
Information Commission (ICO)	UK GDPR and Data Protection Act 2018; supervisory body for UK trust services	UK-wide	ico.org.uk

The UK Accreditation Service accredits the conformity assessment bodies that certify providers; OfDIA must approve a body before it can seek that accreditation.

2

Licensing and authorisation

No licence is needed to sell identity verification in the UK. Instead, Part 2 of the [DUAA](#) creates a statutory scheme that providers join voluntarily, but that other laws increasingly require relying parties to use. Part 2 has been in force since 1 December 2025, apart from sections 45 to 48 [Enacted, not yet commenced](#), which would let public authorities share data with registered providers.

Certification and registration

The Secretary of State must register a provider that holds a certificate from an accredited conformity assessment body confirming its services meet the trust framework, applies in the form OfDIA determines, and pays any fee set by regulations (section 33). A certificate is ignored if it has expired, been withdrawn, or is superseded under transitional rules in a revised framework. Use-case rules sit in supplementary codes, recorded on the register as a "supplementary note" (section 36). Codes currently exist for digital right to work checks, digital right to rent checks and Disclosure and Barring Service identity checks.

Certification is role-based. Version 1.0 of the framework defines identity service providers, attribute service providers, holder service providers (wallets), orchestration service providers and component service providers; a component service cannot be certified alongside any other role.

The move from version 0.4 to version 1.0

The UK digital verification services trust framework 1.0

[Adopted, in force on first accreditation](#) was published on 9 June 2026. It comes into force on the date the first conformity assessment body is accredited to certify against it, which is no earlier than 1 September 2026. GOV.UK records the 1.0.1 certification scheme as live from 2 September 2026, and the 0.4.4 scheme as live until 1 December 2028.

Certificates against version 0.4 stay valid for a transition period: a 0.4-certified service may recertify against 0.4 if it applies within 15 months of 1.0 coming into force, and all 0.4 certificates lapse 27 months after that date.

Consequences of not being registered

Only a registered provider may use the government trust mark (section 50), and registration is now a condition of statutory defences such as the right to work defence.

Identity framework (AML rules do not apply)

Government departments delivering public services, and digital verification services as such, are not "relevant persons" under regulation 8 of the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017. That list covers credit and financial institutions, professional services, estate and letting agents, high value dealers, casinos, art market participants and cryptoasset businesses.

Identity in the public sector is instead governed by three layers:

Statutory trust framework

Rules for certified providers under DUAA Part 2, plus supplementary codes for specific uses. Version 1.0 uses Good Practice Guide 45 (GPG 45) as the required method for identity checking.

GPG 45, "How to check someone's identity"

A scoring method across five checks (strength, validity, activity history, identity fraud, verification) that produces four levels of confidence: low, medium, high and very high.

Use-specific law

Immigration legislation for right to work and right to rent, and licensing law for age checks, which prescribe how checks must be done to give a statutory defence.

Identity verification and onboarding

GOV.UK One Login

Central government services increasingly use GOV.UK One Login. A user proves their identity once and the result is saved to their account for reuse. There are three routes: the GOV.UK One Login app, security questions answered online, or an in-person check at a Post Office that offers in-branch verification.

The app checks that the photo ID is real, that the user is a real person, and that the user matches the ID. With a passport (UK, or non-UK with a biometric chip), biometric residence permit, biometric residence card or Frontier Worker permit, the user photographs the document, reads its chip with the phone and scans their face. With a UK photocard driving licence, there is no chip read. An expired passport is not accepted in the app; a DVLA

driving licence is accepted up to 90 days after expiry, and a residence permit or card up to 24 months after expiry.

How confidence is scored

Under GPG 45 1.0, a UK biometric passport or eVisa record scores 4 for strength, and a UK photocard driving licence scores 3. Reading a document chip and verifying its digital signature reaches validity score 3. For face matching, score 2 requires liveness detection and tests against ISO/IEC 19795-1 and ISO/IEC 30107-1; score 3 adds independent testing by an ISO/IEC 17025 accredited laboratory, a benchmarked algorithm and "enhanced liveness"; and both require defences against replay and injection attacks. A National Insurance number must not be accepted as proof of identity.

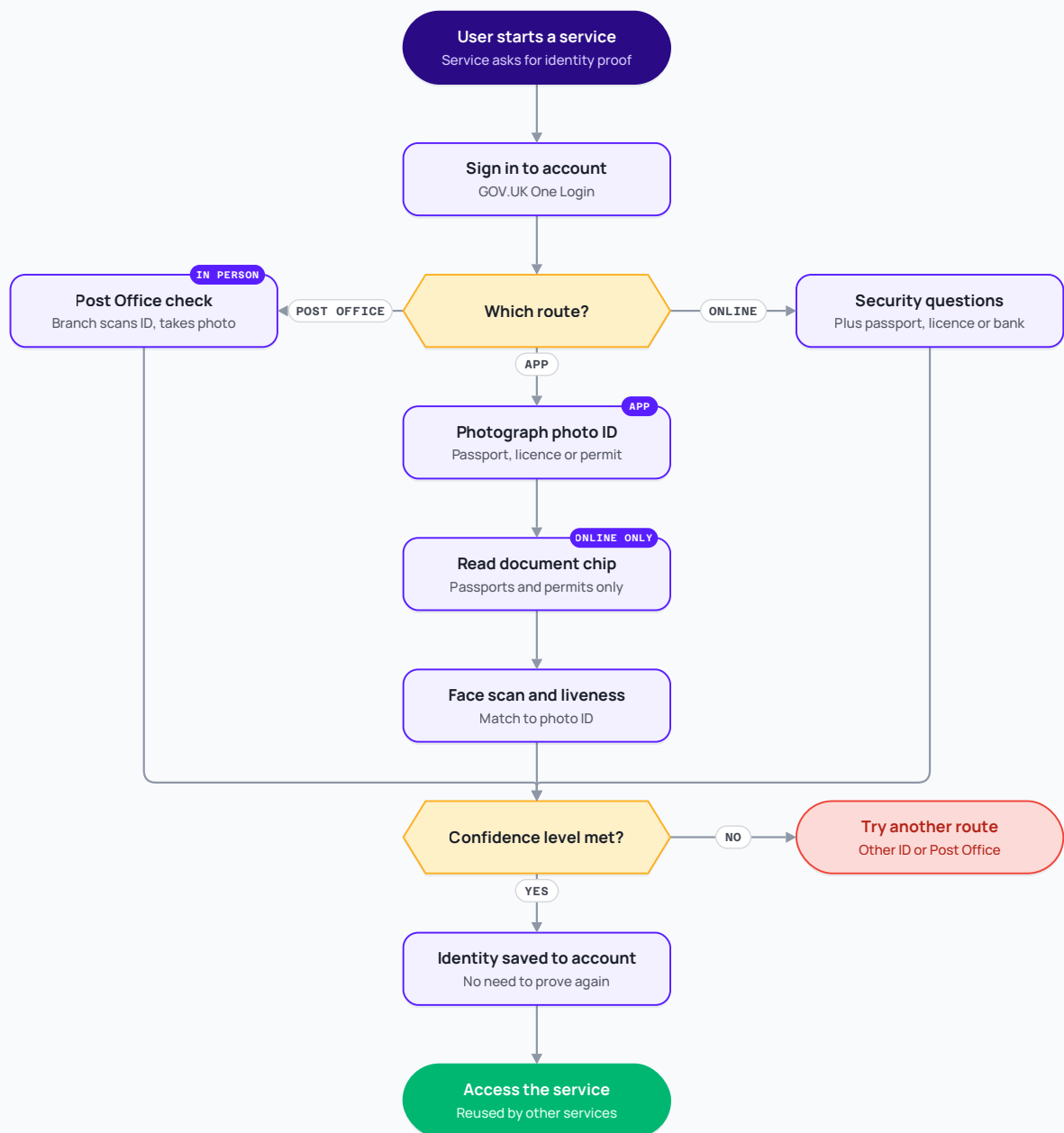


Figure 1. Remote identity proving for a UK public service using GOV.UK One Login.

5

Digital channels: what's different

Bottom line: the scoring method is channel-neutral, but the law now dictates who may run the digital check: from 1 October 2026 a digital right to work check only gives a defence if a registered right to work provider performs it, while the very highest GPG 45 scores remain reserved for supervised in-person checks.

Requirement	In person	Online / remote	Difference
GOV.UK One Login route	Post Office in-branch scan of photo ID and photo	App (document, chip, face) or security questions	Differs
Accepted photo ID for One Login	Includes EU driving licences and EU, Norway, Iceland, Liechtenstein ID cards	App: UK licence, chipped passports, UK residence permits and cards	Differs
Highest GPG 45 validity score (4)	Available with specialist equipment	Not available; maximum 3	Differs
Highest GPG 45 verification score (4)	Available under supervised, controlled conditions	Not available; maximum 3	Differs
British passport for right to work	Manual check: current or expired	Registered provider: current or up to 6 months expired	Differs
Who may perform the check	Employer checks original documents	Registered right to work provider only	Differs
Retention of right to work evidence	Duration of employment plus two years	Duration of employment plus two years	Same
Legal basis for face matching	UK GDPR special category rules	UK GDPR special category rules	Same

Right to work: registered providers only

The Immigration (Restrictions on Employment and Residential Accommodation) (Prescribed Requirements and Codes of Practice) (Amendment) Regulations 2026 (SI 2026/700) replaced the earlier "identity document validation technology" route with checks by a "right to work digital verification service provider" (RtW DVSP): a person on the DVS register with a supplementary note for right to work services. The employer must obtain confirmation of that registration and that the check followed the right to work supplementary code. Where facial recognition is used, including alongside the Home Office online share code check, it must be provided by an RtW DVSP and the employer must keep the facial images and the provider's match confirmation for two years after employment ends. Digital checks remain optional: employers must offer a manual check to anyone who does not want, or cannot use, a digital check.

Remote checks cannot reach every profile

Some very high confidence profiles in GPG 45 (for example V1B and V1D) need a validity or verification score of 4, which can only be achieved in person. Remote services can still reach very high confidence through profiles that combine a strength 4 document with validity 3, verification 3 and a stronger identity fraud check.

Digital ID for age checks

In England and Wales, the Licensing Act 2003 (Mandatory Licensing Conditions) (Amendment) Order 2026 allows age verification policies for alcohol sales to accept identification in digital form through an agreement with a digital verification service provider, from 15 September 2026.

Pending: the Digital Access to Services Bill **Announced, not yet law** would put a voluntary national digital ID on a statutory footing, with digital right to work checks as an early use.

6 Data protection and biometrics

The UK GDPR and the Data Protection Act 2018 apply to every identity check. The Information Commission took over the functions of the Information Commissioner on 30 September 2026, and statutory references in DUAA Part 2 now name the Commission.

ICO guidance on biometric recognition treats face matching for identification or verification as processing special category biometric data. A controller needs a lawful basis and a separate Article 9 condition. Explicit consent is likely to be the most appropriate condition because no specific condition covers identity verification; consent must be freely given, which the ICO says public authorities and employers must consider carefully, and a suitable alternative must be offered to anyone who declines. Without a valid condition, biometric recognition must not be used. The ICO states that this guidance is under review following the 2025 Act.

Retention for right to work evidence is fixed by the Home Office rules: employment plus two years, then secure destruction.

Right to work and right to rent checks

The Home Office employer's guide of 1 October 2026 describes three routes: a manual document check, the Home Office online check using a share code, and a check through an RtW DVSP. An RtW DVSP may check British or Irish passports (or Irish passport cards) up to six months past expiry, using passive authentication of the chip for expired documents, and may verify acceptable documents where the issuing authority makes them available digitally. A clipped passport is cancelled and not acceptable. If an employer buys the service through a screening agency that is not itself certified, the agency must name the registered provider performing the check. The same instrument amends the right to rent rules, which apply in England.

SI 2026/700 also brings contractors and online matching services into the right to work scheme where they arrange work through others, requiring contract terms, audit rights and systems to confirm that the person doing the work is the person who was checked.

Supplementary codes

Version 1.1 of the right to work and right to rent supplementary codes was published on 1 September 2026; the 1.0 versions of those two codes never came into force. Version 0.4 codes remain listed as current. The Disclosure and Barring Service code is at version 1.0, published 9 June 2026.

The national digital ID and GOV.UK Wallet

The Cabinet Office consultation on a national digital ID

Consultation closed, response pending ran from 10 March to 5 May 2026, followed by a People's Panel ending on 21 June. The government says there will be no legal obligation to have or show the digital ID. The consultation states that the GOV.UK Wallet would hold it and is expected to be certified as a DVS. The King's Speech briefing of 13 May 2026 says the Bill would set out the credential's contents, issuing, storage and verification, and an audit function for digital right to work checks, and that most measures would extend to the whole UK.

IDENTITY FRAUD INDICATORS IN PUBLIC-SERVICE AND RIGHT TO WORK CHECKS

- **Synthetic identity:** made-up or part-genuine attributes, including images generated with artificial intelligence.
- **Insider impostor:** someone using non-public data about the claimed identity, such as an HR colleague.
- **Replay or injection attack:** pre-recorded or intercepted images or video fed into a remote check.
- **Presentation attack:** masks, make-up, prosthetics or 3D avatars used to match another person's photo.
- **Deceased identity:** no recent activity history, or authoritative sources show the person has died.
- **Compromised evidence:** a document reported lost, stolen or cancelled, including a clipped passport.
- **National Insurance number offered as proof:** a reference number widely shared and linked to identity fraud.
- **Unnamed provider:** a screening agency that cannot identify the registered provider behind a check.

Right to work. An employer that has not carried out the prescribed checks faces a civil penalty of up to £60,000 per illegal worker; in serious cases a criminal conviction with up to five years in prison and an unlimited fine; business closure and compliance orders; director disqualification; and loss of the ability to sponsor migrants. The Home Office publishes a quarterly list naming employers that have not paid a penalty after exhausting their appeal rights, or that have received a second or further penalty.

DVS register. The Secretary of State may refuse or remove registration for failing to comply with the trust framework or a supplementary code, failing to answer an information notice, or on national security grounds, after notice and at least 21 days for representations. The decision may bar a fresh application for up to two years. Unauthorised use of the trust mark can be stopped by injunction. A certificate from a body not approved by OfDIA is not valid under the scheme.

Data protection. Under section 157 of the Data Protection Act 2018, the higher maximum penalty is £17,500,000 or 4% of an undertaking's worldwide annual turnover, whichever is higher; the standard maximum is £8,700,000 or 2%. Which applies depends on the provision breached.

10 Recent changes and what to watch

- **1 October 2026** **In force** SI 2026/700: digital right to work and right to rent checks must use a registered provider; expired passports up to six months accepted digitally. Review provider contracts and evidence retention.
- **30 September 2026** **In force** The Information Commission replaced the Information Commissioner. Update regulator references in privacy notices.
- **15 September 2026** **In force** Digital ID through a DVS provider can be accepted for alcohol age checks in England and Wales.
- **1 to 2 September 2026** **Adopted, in force on first accreditation** Right to work and right to rent codes 1.1 published; certification scheme 1.0.1 live for trust framework 1.0. Plan the uplift from 0.4.
- **13 May 2026** **Announced, not yet law** Digital Access to Services Bill announced for a voluntary national digital ID. Watch for its introduction to Parliament.
- **10 March to 5 May 2026** **Consultation closed, response pending** National digital ID consultation. The response will set out the credential's content and uses.
- **1 December 2025** **Partly in force** DUAA Part 2 commenced except sections 45 to 48 (public authority data sharing with registered providers).

11 What this means for identity verification

Design for GPG 45 profiles, not for a single document. A chip-read UK passport with a tested face match and liveness check supports medium and high confidence remotely; driving licences without a chip, knowledge-based questions and vouching support lower profiles or combinations. Treat chip reading (NFC) as the main route to validity score 3 online.

For right to work and right to rent, check the provider's DVS register entry and supplementary note before relying on it, record the confirmation in the output, and keep the document image, facial images and match result for employment plus two years. Offer a manual route alongside any digital journey.

Biometric matching needs explicit consent in most cases, with a non-biometric alternative. Test liveness and injection-attack defences against the ISO standards GPG 45 names, and plan for recertification as services move from framework 0.4 to 1.0 within the 27-month window.

IDENTOMAT

How Identomat helps

Identomat runs identity verification, screening and monitoring for regulated businesses on one platform, with workflows you configure for each market. For the requirements in this guide, that means:

- ID document capture and verification, including NFC chip reading of passports and residence permits, to support higher GPG 45 validity scores.
- Face match with biometric liveness detection for remote verification checks.
- Configurable workflows in the no-code workflow builder, with an alternative non-biometric route where consent is declined.
- An audit trail of each check, supporting evidence retention for right to work and right to rent defences.
- Cloud, on-premises or hybrid deployment for public-sector data residency needs.

[Request a meeting](#)

DISCLAIMER

This article is intended for informational purposes only and does not constitute legal advice. It is a compilation of information from various sources and reflects the information available as of the last updated date indicated above. Laws, regulations, and regulatory guidance may change, so readers should consult qualified legal professionals for advice specific to their circumstances.

Sources

- Data (Use and Access) Act 2025, Part 2 (sections 27 to 55), with commencement information, [legislation.gov.uk](https://legislation.gov.uk/ukpga/2025/18/part/2), legislation.gov.uk/ukpga/2025/18/part/2
- UK digital verification services trust framework (1.0), OfDIA, published 3 March 2026, final release 9 June 2026, section 0, gov.uk

- **UK digital verification services trust framework collection (current versions 1.0 and 0.4)**, OfDIA, updated 11 June 2026, gov.uk
- **Certification scheme for the UK digital verification services trust framework**, OfDIA, updated 21 September 2026, gov.uk
- **Supplementary codes for digital verification services**, OfDIA, updated 1 September 2026, gov.uk
- **Join the digital verification services register**, OfDIA, updated 1 December 2025, gov.uk
- **How to check someone's identity (1.0) (GPG 45)**, OfDIA, updated 9 June 2026, sections 3, 5, 6, 9, 12.3 and Appendix 4, gov.uk
- **Using your GOV.UK One Login: Proving your identity**, Government Digital Service, gov.uk
- **Proving your identity with the GOV.UK One Login app**, Government Digital Service, updated 25 June 2026, gov.uk
- **The Immigration (Restrictions on Employment and Residential Accommodation) (Prescribed Requirements and Codes of Practice) (Amendment) Regulations 2026 (SI 2026/700)**, in force 1 October 2026, legislation.gov.uk
- **Right to work checks: an employer's guide (1 October 2026)**, UK Visas and Immigration and Immigration Enforcement, sections on RtW DVSP checks and sanctions, gov.uk
- **Digital right to work and rent checks for British and Irish citizens: equality impact assessment**, Home Office, 30 June 2026, gov.uk
- **Illegal working penalties: UK report**, UK Visas and Immigration and Immigration Enforcement, gov.uk
- **Making public services work for you with your digital identity**, Cabinet Office consultation, 10 March to 5 May 2026, gov.uk
- **King's Speech 2026: background briefing notes**, Prime Minister's Office, 13 May 2026 (updated 28 May 2026), Digital Access to Services Bill, pp. 79 to 80, gov.uk
- **The Licensing Act 2003 (Mandatory Licensing Conditions) (Amendment) Order 2026 (SI 2026/1022)**, in force 15 September 2026, England and Wales, legislation.gov.uk
- **The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017, regulation 8**, legislation.gov.uk
- **Data Protection Act 2018, section 157 (maximum amount of penalty)**, legislation.gov.uk
- **The Electronic Identification and Trust Services for Electronic Transactions Regulations 2016 (SI 2016/696)**, regulation 3, legislation.gov.uk
- **Biometric data guidance: How do we process biometric data lawfully?**, ICO, ico.org.uk