Identomat

COMPLIANCE GUIDE

Government & Public Services Compliance in Australia

COUNTRY Australia

INDUSTRY Government & Public Services

LAST UPDATED 2 November 2026

KEY REGULATORS Australian Competition and Consumer Commission (Digital ID Regulator) · Office of the Australian Information Commissioner · Attorney-General's Department

Key takeaways

- Australia's national digital identity rules sit in the Digital ID Act 2024 and its rules. Accreditation as a Digital ID provider is voluntary, but it is mandatory for any provider that wants to join the Australian Government Digital ID System (AGDIS), the federal network that myID and government online services use.
- Until 30 November 2026 only Commonwealth, state and territory bodies can apply to join AGDIS. From 1 December 2026, two years after the Act commenced, private businesses and accredited private providers can apply automatically under the Act itself; no further instrument is needed.
- Identity strength is graded on six identity proofing levels. From the "IP2 Plus" level upward the person's face must be matched to a verified photo ID, and online this must happen in one continuous session with liveness detection tested against an international standard (ISO/IEC 30107).
- A service that accepts a Digital ID through AGDIS must also offer a reasonably accessible way in that does not need one. Private businesses can ask for an exemption; Commonwealth agencies and entities cannot.
- Face images and other biometrics collected only to verify identity must be destroyed immediately after the check. One-to-many face searching is banned for accredited providers, with civil penalties of up to 1,500 penalty units per breach (five times that for companies).

Australia is open to digital identity providers, but the trusted government network is still being phased in. As at 2 November 2026 all 40 entities on the AGDIS register are public bodies; private relying parties and private identity providers can apply from 1 December 2026. Outside AGDIS, private providers may seek accreditation voluntarily and are then bound by the same privacy and biometric safeguards; three private companies held accreditation at that date. State and territory agencies add their own identity schemes and privacy laws, which differ markedly between jurisdictions.

The principal regulators are the Australian Competition and Consumer Commission (ACCC), acting as Digital ID Regulator, and the Office of the Australian Information Commissioner (OAIC), which enforces the privacy safeguards. The Attorney-General's Department runs the separate Document and Face Verification Services that most remote proofing relies on.

The biggest obstacle for a new entrant is the accreditation burden: protective security, fraud control, privacy impact assessment, accessibility testing and, for biometric binding, independent laboratory testing of presentation attack detection before the regulator will accredit.

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

Digital identity is governed at the Commonwealth level: the Digital ID Act 2024 names the regulator and system operator (ss 90 and 94), and the Identity Verification Services Act 2023 governs the government document and face matching services.

Authority	Remit	Level	Official site
Australian Competition and Consumer Commission (Digital ID Regulator)	Accredits providers, approves AGDIS participation, keeps the accredited entities and AGDIS registers, enforces the Act	Commonwealth	accc.gov.au
Office of the Australian Information Commissioner	Privacy regulator for the Digital ID system; enforces the Act's privacy safeguards; assesses the identity verification facilities each year	Commonwealth	oaic.gov.au
System Administrator (Chief Executive Centrelink, Services Australia)	Day-to-day operation of AGDIS, incident handling, redress directions	Commonwealth	Digital ID Act s 94

Minister for Finance	Makes the Digital ID Rules, Accreditation Rules and phasing-in determinations; sets AGDIS policy	Commonwealth	Explanatory statement
Attorney-General's Department	Operates the Document Verification Service (DVS), Face Verification Service (FVS) and Face Identification Service under the IVS Act	Commonwealth	idmatch.gov.au

myID is administered by the Australian Taxation Office (ATO) and is accredited under s 15 of the Digital ID Act. State and territory departments, and companies they own, may join AGDIS under the Phasing-in Determination 2024; they also issue the driver licences and other documents that the DVS checks.

State and territory layer

State and territory agencies follow their own identity schemes and privacy laws, which differ materially. Victoria has its own four-level assurance framework (LOA1 to LOA4); New South Wales is piloting a Digital ID at IP3; digital driver licences have legal footing in New South Wales, Victoria, Queensland and South Australia only. Agencies in every jurisdiction act as AGDIS relying parties. For DVS and FVS access, the IVS Rules 2024 recognise every state privacy law except those of Western Australia and South Australia, whose agencies must agree to the Australian Privacy Principles instead. Tax file number breaches by any state agency are notifiable to the OAIC (Privacy Act 1988 ss 11 and 26WE(1)(d)).

Jurisdiction	State identity scheme or credential	Privacy law for state agencies	Biometrics listed as sensitive	Breach notification in the Act
New South Wales	NSW Digital ID pilot (Service NSW, IP3, facial verification); digital driver licence usable as evidence of identity (Road Transport Act 2013 s 61C)	Privacy and Personal Information Protection Act 1998	No	Yes, Part 6A (from 28 Nov 2023)

Victoria	Service Victoria Identity Verification Standards, version 7 (15 Oct 2026), made under Service Victoria Act 2018 s 41: LOA1 to LOA4, LOA3 needs a photo bind, LOA4 an in-person biometric check; digital driver licence since 3 Apr 2025 (S.R. No. 15/2025)	Privacy and Data Protection Act 2014	No	No
Queensland	Digital authority, digital evidence of age and digital evidence of identity displayed in an approved app (Transport Planning and Coordination Act 1994 Part 4E, ss 29AE to 29AI)	Information Privacy Act 2009 (Queensland Privacy Principles)	Yes	Yes, Chapter 3A
Western Australia	No digital licence provision in the Road Traffic (Authorisation to Drive) Act 2008 (as at 28 Oct 2026); digital licence and State Digital Identity funded, licence expected by end of 2027; AGDIS relying party	Privacy and Responsible Information Sharing Act 2024 (principles from 1 Jul 2026)	Yes	From 1 Jan 2027 (Part 2 Division 6)
South Australia	Digital licence in the mySA GOV app; Motor Vehicles Act 1959 s 5(5) allows licences in electronic form; AGDIS relying party	No privacy Act; Information Privacy Principles Instruction (Cabinet Administrative Instruction 1/89, PC012)	Not addressed	Not addressed

Tasmania	No digital licence provision in the Vehicle and Traffic Act 1999; AGDIS relying parties	Personal Information Protection Act 2004	No	No
Australian Capital Territory	No digital licence provision in the Road Transport (Driver Licensing) Act 1999 or its Regulation; AGDIS relying party	Information Privacy Act 2014	Yes	No; TFN breaches notifiable to the OAIC, which receives ACT agency breach notifications by arrangement
Northern Territory	No digital licence provision in the Motor Vehicles Act 1949 (as in force 18 Nov 2025); digital licence announced for late 2026; AGDIS relying party	Information Act 2002	No	No

2 Licensing and authorisation

Accreditation In force

Under s 14 of the Digital ID Act 2024 (Compilation No. 2, 21 February 2025), Australian bodies corporate, registered foreign companies, Commonwealth entities and state or territory departments may apply to the ACCC for accreditation as an identity service provider (ISP), attribute service provider or identity exchange provider. Accreditation is voluntary unless the provider wants to operate inside AGDIS. Applicants must meet the Digital ID (Accreditation) Rules 2024 (Compilation No. 1, 19 November 2025), which require a privacy impact assessment, protective security and fraud control capabilities, penetration testing, useability and accessibility (WCAG) testing, and an assessor's report. Accredited entities then file annual reports and repeat testing. The ACCC register lists five accredited entities as at 2 November 2026: the Commissioner of Taxation (myID), Services Australia, ConnectID Pty Ltd, Makesure Consulting Pty Ltd and OCR Labs Pty Ltd (IDVerse). Holding out that an entity is accredited when it is not carries a civil penalty of 1,000 penalty units (s 31).

Approval to participate in AGDIS

Section 59 allows an entity to provide or receive services within AGDIS only if it holds an approval under s 62 and its participation start day has arrived. A relying party must be an Australian entity or a registered foreign company; identity and attribute providers must also be accredited. Operating in the system without meeting these conditions attracts 1,000 penalty units.

Section 61 controls who may apply. Commonwealth relying parties and accredited non-corporate Commonwealth entities may apply now; state and territory bodies are admitted by the Phasing-in Determination 2024 (F2024L01437), made under s 60. Any accredited entity, accreditation applicant, Australian relying party or registered foreign company may apply once more than two years have passed since the Act commenced on 30 November 2024, that is from 1 December 2026 (s 61(d)) `Adopted, effective 1 Dec 2026`. The Minister for Finance announced on 26 June 2026 that higher-risk government services will not accept private provider Digital IDs and that business relying parties will pay from 1 January 2027 at the latest.

Government verification services

Access to the DVS and FVS requires a participation agreement under the IVS Act 2023 (Compilation No. 1, 11 December 2024). Businesses reach the DVS only through an approved gateway service provider, which sets its own charges. The Attorney-General's Department's agreements register lists 2,431 agreements in force (2,266 private sector); only two are face matching agreements, both with Commonwealth agencies (the ATO and the Department of Foreign Affairs and Trade).

3 Identity framework (AML rules do not apply)

Public bodies delivering public services are not reporting entities under the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Compilation No. 63, 1 October 2026), because the Act applies to persons providing the financial, bullion, gambling, real estate, professional and prescribed "designated services" listed in s 6.

Identity in this sector is governed instead by three layers:

Digital ID Act 2024

Accreditation, AGDIS participation, extra privacy safeguards, voluntary use and redress.

Accreditation Rules and Data Standards

Proofing levels, biometric binding, authenticators and biometric testing.

IVS Act 2023

Consent and privacy conditions for DVS and FVS checks.

4 Identity verification and onboarding

Identity proofing levels

Rule 5.10 of the Accreditation Rules sets six identity proofing (IP) levels: IP1, IP1 Plus, IP2, IP2 Plus, IP3 and IP4. Every level above IP1 requires uniqueness checks, checks against known fraudulent identities, and verification of name and date of birth only by source verification (with the issuer or a service such as the DVS) or technical verification (public key cryptography). The main steps up:

Level	Credentials	Biometric binding	Authenticator
IP1	None verified (self-asserted)	No	AL1, AL2 or AL3
IP1 Plus	Photo ID or a "use in the community" credential	No	AL2 or AL3
IP2	Commencement-of-identity credential or photo ID, plus use in the community; linking credential if names differ	No	AL2 or AL3
IP2 Plus	Photo ID plus use in the community	Required	AL2 or AL3
IP3	Commencement of identity, photo ID and use in the community; deceased-person check required	Required	AL2 or AL3

IP4	Commencement of identity, photo ID and two use-in-the-community credentials; originals presented and the person witnessed in person	Required	AL3

An Australian passport can satisfy both the commencement-of-identity and photo ID requirements at IP3, but only one of them at IP4 (rule 5.11). Technical verification of an Australian passport or foreign ePassport must follow ICAO Doc 9303 and check the issuer's certificate revocation list (rule 5.12). A foreign passport used for biometric binding must first be linked to a source-verified visa (rule 5.16). An ISP must not create a Digital ID for anyone under 15 (rule 5.2).

How myID applies the levels

myID, the Australian Government's Digital ID app, presents three identity strengths: Basic, Standard and Strong. Strong requires at least two verified documents and a verified photo, matched to an Australian passport (or, in combination with other documents, a Western Australian driver licence). Each government online service sets its own minimum; the myID service list shows Standard for myGov, Centrelink and director ID, and Strong for a tax file number application.

Reliance on government verification services

The DVS returns only a match or no-match result against issuer records, and the FVS (one-to-one face matching) returns only a match result to non-government users; facial images are never sent to them (IVS Act ss 15 and 19). Each check needs the individual's express consent under the participation agreement (s 9), and the DVS should not be the sole basis for a decision to provide a service. In 2024-25 the DVS was used 133,140,077 times by 2,228 entities, 2,109 of them private sector; the FVS was used by one government agency only.

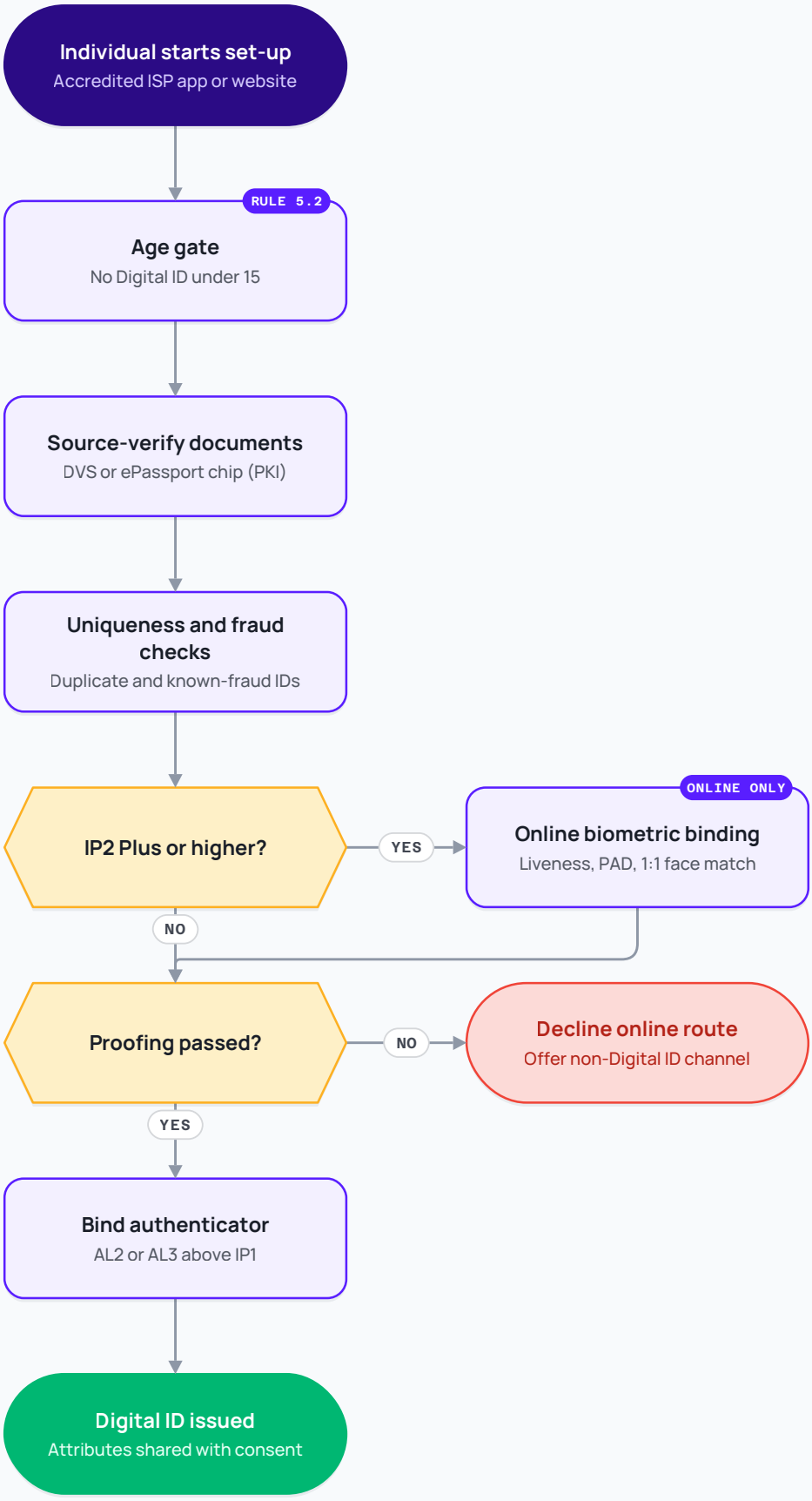


Figure 1. Remote identity proofing by an accredited identity service provider in Australia.

5 Digital channels: what's different

Bottom line: the privacy and biometric safeguards are channel-neutral, but online biometric binding carries extra technical duties (single session, liveness, independently tested presentation attack detection), and the highest level, IP4, is available only in person.

Requirement	In person	Online / remote	Difference
Highest proofing level available	IP4 (originals, witnessed)	IP3	Differs
Face match method	Technical, source or eIDVT matching; manual comparison by a trained officer if none is available	Technical, source or eIDVT matching only; no manual comparison	Differs
Liveness and presentation attack detection	Assessing officer present	Mandatory at capture, single continuous workflow	Differs
Independent biometric testing	Not required for manual comparison	PAD tested by an ISO/IEC 17025 lab against ISO/IEC 30107-3	Differs
Alternative to Digital ID (AGDIS relying parties)	Is itself an alternative route	Must be backed by a reasonably accessible non-Digital ID route; no exemption for Commonwealth bodies	Differs
Biometric destruction after verification	Immediately after the check	Immediately after the check	Same
Consent for DVS and FVS checks	Express consent	Express consent	Same
Ban on tracking which services a user accesses	Applies	Applies	Same

Online biometric binding

Rule 5.17 requires online binding to capture an image, apply an image quality profile informed by ISO/IEC 29794-5, and run technical, source or (at IP2 Plus only) eIDVT matching. The whole process must run in a single continuous workflow, with liveness detection as part of presentation attack detection (PAD) at the point of capture, using technology that meets ISO/IEC 30107-1.

Document authenticity checks from a phone camera

Biometric matching through electronic identity document verification technology (eIDVT), permitted only at IP2 Plus, may use only a driver licence, a state or territory proof-of-age card or an Australian passport physically presented to a camera. Rule 5.20 requires document liveness testing, checks of at least five security features, at least 300 dpi, at most five attempts, no manual review and immediate destruction of the images.

Testing standard

Under s 2.3 of the Digital ID (Accreditation) Data Standards 2024, PAD for online binding must be tested by an independent laboratory with at least six low-effort and six moderate-effort attack types and ten test subjects, and an attack presentation classification error rate (APCER) of 0%.

Voluntary use

Section 74 bars participating relying parties from requiring a Digital ID; the alternative must be reasonably accessible and not substantially less favourable. Private relying parties may seek an exemption, for example if they operate solely online; Commonwealth entities, Commonwealth companies and agencies under the Freedom of Information Act 1982 cannot (s 74(6)).

6 Data protection and biometrics

The Privacy Act 1988 applies to agencies and most businesses; the Digital ID Act adds safeguards for accredited entities, some of which consent cannot override.

- **Biometrics (ss 48 to 51).** Collection only with express consent, only to verify identity or authenticate the user, and only if the accreditation conditions authorise it. One-to-many matching, and using biometrics to detect multiple Digital IDs, are prohibited. Data collected only to verify identity must be destroyed immediately after verification; testing and fraud-investigation copies within 14 days at most.

- **Prohibited attributes (s 44).** Providers must not collect information about racial or ethnic origin, political or religious views, philosophical beliefs or sexual orientation.
- **No profiling (s 53).** Information about which services a person accessed, how or when, cannot be used or disclosed even with consent, except for system performance, compliance with the Act or as required by law.
- **Records.** AGDIS identity and attribute providers keep prescribed records for three years from creation or last use, whichever is later (Digital ID Rules 2024, rule 6.2).

FVS users must destroy facial images created for a request once no longer needed (IVS Act s 10). For state agencies, the state privacy law in section 1 applies instead of the Privacy Act. The OAIC's guide on facial recognition (updated 29 July 2026) confirms that biometric templates and facial images used for automated verification are sensitive information and recommends a privacy impact assessment before deployment.

7 Sector-specific obligations

Incident reporting

Entities in AGDIS must notify cyber security and Digital ID fraud incidents to the System Administrator as soon as practicable and no later than one business day after becoming aware or suspecting one; an oral notice must be confirmed in writing within three business days (Digital ID Rules 2024, rule 4.2).

Redress for affected users

Chapter 4A of the Digital ID Rules requires AGDIS identity and attribute providers to make reasonable attempts to notify each individual affected by an incident and to give information, support and assistance. Since 30 September 2026 the System Administrator may also direct a provider to apologise or explain, and recommend compensation.

Accessibility and inclusion

Accredited entities must take reasonable steps to make services accessible to people facing barriers (s 30). Where its accreditation conditions allow, an ISP may use an alternative proofing process, such as other credentials or a verified trusted referee (rule 5.23).

8 Risk indicators and red flags

IDENTITY FRAUD INDICATORS IN REMOTE PROOFING

- **Presentation attacks**: printed photos, screen replays or masks presented to the camera instead of a live face.
- **Second-generation document images**: photos of a screen or photocopy, or previously captured images, submitted as an original ID.
- **Duplicate identities**: the same person or the same documents used to create more than one Digital ID.
- **Deceased-person identities**: credentials of a deceased individual (check mandatory from IP3).
- **Name or date of birth variance**: details that differ across documents without a linking credential.
- **Unlinked foreign passports**: a foreign passport not tied to a verified visa.
- **Cancelled passports**: an ePassport listed on the issuer's certificate revocation list.
- **Repeated attempts**: more than five eIDVT attempts to authenticate the same photo ID.

9 Enforcement and penalties

The Digital ID Act is enforced through civil penalties, infringement notices, enforceable undertakings, directions and suspension or revocation of accreditation; the ACCC applies for most penalties and the Information Commissioner for the privacy safeguards (s 123). Penalties are set per contravention in penalty units, and a court may order a body corporate to pay up to five times the stated amount (Regulatory Powers (Standard Provisions) Act 2014, s 82(5)). The Commonwealth penalty unit, indexed under s 4AA of the Crimes Act 1914, is $364 from 1 July 2026 (previously $330); the dollar figures below use $364.

Contravention	Provision	Maximum (individual)	Maximum (body corporate)

Biometric collection, retention, destruction; prohibited attributes; profiling; offshore data rules; reportable incidents	ss 44 to 56, 77, 78	1,500 units ($546,000)	7,500 units ($2.73 million)
Holding out as accredited; operating in AGDIS without approval; breaching directions or record keeping	ss 31, 59, 83, 127 to 130, 133 to 136	1,000 units ($364,000)	5,000 units ($1.82 million)
Unauthorised use or disclosure by entrusted persons	s 151 (offence)	2 years' imprisonment or 120 units, or both	

The ACCC's first Digital ID Regulator annual report (period to 30 June 2025) records 19 investigations commenced, four closed and three matters resolved administratively; two of these required relying parties to restore a reasonably accessible non-Digital ID route under s 74. The System Administrator received 194 fraud incident notifications affecting 763 Digital IDs. As at November 2026 the Federal Court had published no judgment under the Digital ID Act or the IVS Act.

Oversight of the government verification services runs through the OAIC's annual assessments under s 40 of the IVS Act. Its first report (20 December 2024) found the FVS managed in line with privacy requirements apart from two medium-risk gaps, and made two recommendations.

10 Recent changes and what to watch

- **1 January 2027, Western Australia breach scheme** `Adopted, effective 1 Jan 2027`: WA public entities must notify notifiable information breaches under the Privacy and Responsible Information Sharing Act 2024.
- **10 December 2026, automated decision disclosures** `Adopted, effective 10 Dec 2026`: privacy policies must explain where computer programs make or substantially inform significant decisions, which can include automated identity checks.
- **1 December 2026, AGDIS opens to private applicants** `Adopted, effective 1 Dec 2026`: businesses and accredited private providers can apply under s 61(d); business charges start by 1 January 2027.
- **15 October 2026, Service Victoria standards version 7** `In force`: revised Victorian identity verification standards (LOA1 to LOA4).

- **30 September 2026, Redress Framework Rules 2026** `In force`: tighter user notification duties and System Administrator powers to direct apologies and recommend compensation.
- **29 July 2026, OAIC facial recognition guide** `Published guidance`: updated consent, necessity and privacy impact assessment guidance.
- **1 July 2026, penalty unit, incident policies and WA privacy principles** `In force`: the penalty unit rose to $364, AGDIS incident and complaint policy duties began, and WA's information privacy principles took effect.

11 What this means for identity verification

- **Design to a named level.** Map each service to an IP and authenticator level; claiming a higher level's equivalence is not permitted.
- **Source or cryptographic verification.** Name and date of birth must be verified with the issuer (DVS) or by ePassport chip, not by optical reading alone, at every level above IP1.
- **Liveness for remote binding.** Capture, quality scoring, liveness and PAD in one session, backed by an ISO/IEC 30107-3 test report.
- **One-to-one only.** Duplicate detection by face search is prohibited for accredited entities.
- **Zero retention by default.** Destroy biometric data and processed document images immediately after the check, keeping only fraud or testing copies for up to 14 days where the rules allow.
- **Keep a non-digital route.** Commonwealth services in AGDIS cannot be exempted from offering an accessible alternative.

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 reading of ePassport chips, for source and technical credential checks.
- Biometric liveness and one-to-one face match in a single continuous capture flow, as remote biometric binding requires.
- Configurable no-code workflows to map each service to its required identity proofing level, with assisted and in-person alternatives.
- Cloud, on-premises or hybrid deployment to fit public-sector data location and security requirements.
- An audit trail for each check to support incident reporting and annual review obligations.

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

- **Digital ID Act 2024** (C2024A00025), Compilation No. 2, 21 February 2025 (C2025C00160), ss 2, 14, 15, 30, 31, 44 to 56, 58 to 62, 74, 77, 90, 94, 123, 151, Federal Register of Legislation, legislation.gov.au
- **Digital ID (Accreditation) Rules 2024** (F2024L01438), Compilation No. 1, 19 November 2025 (F2025C01255), rules 5.2, 5.10 to 5.21, 5.23, legislation.gov.au
- **Digital ID (Accreditation) Data Standards 2024** (F2024L01435), ss 2.2 to 2.4, legislation.gov.au
- **Digital ID Rules 2024** (F2024L01430), Compilation No. 2, 30 September 2026 (F2026C00975), rules 4.2, 4A.1 to 4A.8, 6.2, 7.1, 7.2, legislation.gov.au

- **Digital ID (Phasing-in of Participation in the Australian Government Digital ID System) Determination 2024** (F2024L01437), legislation.gov.au
- **Explanatory Statement, Digital ID (Accreditation) Amendment (PSPF and Other Measures) Rules 2025** (F2025L01394), registered 18 November 2025, legislation.gov.au
- **Explanatory Statement, Digital ID Amendment (Redress Framework) Rules 2026** (F2026L00696), registered 15 June 2026, legislation.gov.au
- **Identity Verification Services Act 2023** (C2023A00115), Compilation No. 1, 11 December 2024 (C2024C00830), ss 9, 10, 15, 19, 40, legislation.gov.au
- **Identity Verification Services Rules 2024** (F2024L00625), Compilation No. 1, 7 June 2025, s 5, legislation.gov.au
- **Anti-Money Laundering and Counter-Terrorism Financing Act 2006** (C2006A00169), Compilation No. 63, 1 October 2026, s 6, legislation.gov.au
- **Regulatory Powers (Standard Provisions) Act 2014** (C2014A00093), Compilation No. 4, s 82, legislation.gov.au
- **Crimes Act 1914** (C1914A00012), compilation of 27 August 2026, s 4AA, legislation.gov.au
- **Crimes (Amount of a Penalty Unit) Instrument 2026** (F2026N00424), s 5, legislation.gov.au
- **Service Victoria Act 2018** (Vic), version 066, 21 May 2025, ss 41 to 43, legislation.vic.gov.au; **Service Victoria Identity Verification Standards**, version 7 (15 October 2026), service.vic.gov.au
- **Privacy and Data Protection Act 2014** (Vic), version 034, 30 September 2026, Sch 1, legislation.vic.gov.au
- **Road Transport Amendment (Digital Licensing) Act 2020** (NSW) No 27, s 61C, legislation.nsw.gov.au; **Service NSW, NSW Digital ID terms and conditions** (9 September 2026), service.nsw.gov.au
- **Privacy and Personal Information Protection Act 1998** (NSW), version current from 30 September 2026, s 19, Part 6A, legislation.nsw.gov.au; **Privacy and Personal Information Protection Amendment Act 2022** No 74, s 2, legislation.nsw.gov.au
- **Transport Planning and Coordination Act 1994** (Qld), current as at 21 September 2026, Part 4E, legislation.qld.gov.au; **Information Privacy Act 2009** (Qld), current as at 29 October 2026, Ch 3A, Sch 5, legislation.qld.gov.au
- **Privacy and Responsible Information Sharing Act 2024** (WA), as at 1 July 2026, s 4, Part 2 Division 6 and uncommenced provisions table, legislation.wa.gov.au
- **PC012 Information Privacy Principles (IPPS) Instruction** (SA), Cabinet Administrative Instruction 1/89, approved 4 May 2020, archives.sa.gov.au
- **Personal Information Protection Act 2004** (Tas), s 3, legislation.tas.gov.au; **Information Privacy Act 2014** (ACT), republication 13, 16 December 2025, legislation.act.gov.au; **Information Act 2002** (NT), as in force 1 June 2026, legislation.nt.gov.au
- **Privacy Act 1988** (Cth), Compilation No. 104, 4 June 2026, ss 11 and 26WE, legislation.gov.au; **OAIC, Privacy in the ACT**, oaic.gov.au

- **Road Safety (Drivers) and (General) Amendment (Digital Driver Licence) Regulations 2025** (Vic), S.R. No. 15/2025, legislation.vic.gov.au
- **Road Traffic (Authorisation to Drive) Act 2008** (WA), as at 28 October 2026, legislation.wa.gov.au; **ServiceWA app: Digital driver licence and digital wallet** (updated 22 June 2026), wa.gov.au
- **Motor Vehicles Act 1959** (SA), version 24 November 2025, s 5, legislation.sa.gov.au; **Service SA, Go digital with a digital licence**, service.sa.gov.au
- **Vehicle and Traffic Act 1999** (Tas), legislation.tas.gov.au; **Road Transport (Driver Licensing) Act 1999** (ACT), republication 43, and **Regulation 2000**, republication 83, legislation.act.gov.au; **Motor Vehicles Act 1949** (NT), as in force 18 November 2025, legislation.nt.gov.au; **Service NT, Digital driver licence**, service.nt.gov.au
- **ACCC, Digital ID regulation** (updated 21 July 2026), accc.gov.au
- **ACCC, Digital ID Regulator Annual Report 2024-25** (October 2025, published 23 January 2026), accc.gov.au
- **Digital ID Accredited Entities Register** and **Australian Government Digital ID System Register** (viewed 2 November 2026), accc.gov.au
- **Minister for Finance, Digital ID expands to the private sector** (media release, 26 June 2026), ministers.finance.gov.au
- **myID, Terms of use** (updated 5 October 2026), myid.gov.au
- **myID, Verifying your ID in myID** (updated 9 December 2025) and **Online services you can use** (published 28 October 2024), myid.gov.au, myid.gov.au
- **IDMatch, Become a DVS business user**, Attorney-General's Department, idmatch.gov.au
- **Attorney-General's Department, Identity Verification Services Act 2023 Annual Report 2024-25** (3 March 2026), ag.gov.au
- **Attorney-General's Department, IVS Agreements Register** (viewed 2 November 2026), ivsregister.ag.gov.au
- **OAIC, Facial recognition technology: a guide to assessing the privacy risks** (updated 29 July 2026), oaic.gov.au
- **OAIC, New resources on transparency for use of AI and automated decision-making** (30 September 2026), oaic.gov.au
- **OAIC, Identity Verification Services Assessment Report: Privacy Obligations** (20 December 2024), oaic.gov.au