



Privacy Notice

This privacy notice describes how we (the Department of Home Affairs) collect, use and disclose your personal information to provide the Identity Matching Services (the Services).

The purpose and scope of the Services are set out in the 2017 [Intergovernmental Agreement on Identity Matching Services](#) that was endorsed by all the governments on the Council of Australian Governments.

We manage the Services on behalf of all participating government agencies. We only collect, use and disclose personal information that is reasonably necessary for us to provide the Services.

We are committed to protecting the privacy and security of your personal information in accordance with the *Privacy Act 1988* (Cth) (the Privacy Act). For information on how we generally handle personal information, see the Department of Home Affairs' [privacy policy](#).

The Identity Matching Services

The Identity Matching Services are:

The **Document Verification Service (DVS)** matches a document presented as proof of identity against those held by the originating agency, usually with the person's consent;

The **Face Verification Service (FVS)** compares a person's photo against a government-issued identity document. This is called a 'one-to-one' check and helps to confirm the identity of a known person; and

The **Face Identification Service (FIS)** compares a person's photo against images in multiple government records to help establish their identity or to detect multiple fraudulent identities. This is called a 'one-to-many' check and helps to identify an unknown person. The FIS can only be used by national security, law enforcement and anti-corruption agencies under limited circumstances, as authorised by law.

The hubs

The Identity Matching Services use secure online hubs that operate 24 hours a day, seven days a week. These are technical systems that send information between the organisation requesting to use the service and the agency holding the information used on your government-issued identity document.

The hubs do not retain any personal information and we cannot view or edit any of the personal information transmitted through the hubs. We do store audit information (such as date / time / purpose of match request) that helps to ensure the Services are being used properly. This information is kept for the minimum amount of time needed for auditing purposes.

How your information is collected

A government agency or a business can collect your personal information, in accordance with the Privacy Act. This includes any of the following types of information:

- biographic information, such as name, address, date of birth, and gender;
- visa and citizenship information, including visa or citizenship status and country of citizenship;
- driver licence information, including licence number and licence type (e.g. motor vehicle);
- passport information, including nationality, passport number and expiry date;
- birth information, such as a birth certificate number;
- Medicare information, such as a Medicare card number; and
- facial images.

Your facial image may be used to create a biometric template that is a unique numerical sequence that represents the facial image. Facial recognition software compares biometric templates, not facial images. A facial image cannot be recreated from a biometric template.

State and territory laws also enables collection of information (which includes creation of biometric templates) found on driver licences (including learner permits) and other types of identity documents, such as proof of age cards. Currently, these laws are:

- New South Wales -
s.271A Road Transport Act 2013 (NSW)
- Victoria
s.90k(a)(vi) Road Safety Act 1986
- Queensland
Part 4D Transport Planning and Coordination Act 1994
- South Australia
s.13 Public Sector (Data Sharing) Act 2016
- Tasmania
Regulation 125(2)(da) Vehicle and Traffic (Driver Licensing and Vehicle Registration) Regulations 2010.
- Northern Territory
Regulation 15(1) Motor Vehicles Regulations 1977
- Western Australia
Regulation 160 of Vehicle and Traffic Regulations 2021

How we use your information

We use your biographic and biometric information to provide the Services. The Services are the Document Verification Service (DVS), the Face Verification Service (FVS) and the Face Identification Service (FIS).

The FVS and the FIS CANNOT be used to:

- conduct 'real-time monitoring' or 'live facial recognition' of people in public spaces – sometimes referred to as 'mass surveillance', or
- identify people to investigate minor offences, such as jaywalking or littering.

Documents that can be verified

Identity documents that can be verified through the DVS include:

- birth certificates;
- Centrelink concession cards;
- certificates of registration by descent;
- change of name certificates;
- citizenship certificates;
- driver licences (including learner permits);
- ImmiCards*;
- marriage certificates;
- Medicare cards;
- Australian passports*;
- visas*;
- Death Certificates;
- Aviation and Maritime Security Identification Cards (ASIC/MSIC); and
- Address Details from the Australian Electoral Commission (AEC)**.

* The FIS and the FVS can check facial images on these identity documents.

** This document type is only available to selected organisations, and only for *Anti-Money Laundering and Counter Terrorism Financing Act 2006* (Cth) or *Financial Transaction Reports Act 1988* (Cth) purposes.

What happens to matching data

When an organisation verifies or identifies you, it is requesting a match between the information it has about a person and the information a government agency has on that person.

After the matching request is complete we delete the information from our system. We cannot view or edit the information at all. The government agencies that issued your original identity document will continue to hold your personal information.

The organisation that verifies or identifies you, might still keep the information they collected. If personal information is obtained by a government agency either via a query or in a response to a matching request, the agency must comply with any laws that require the

retention of such information for a specific period of time, and delete the information after that period has expired.

We store audit information (such as date / time / purpose of match request) to ensure the Services are being used properly. This information is kept for the minimum period required by the *Archives Act 1983* (Cth).

How we use your driver licence information

Information on driver licences is handled differently to other information. Information provided by driver licencing authorities is stored in one of two systems.

The [National Exchange of Vehicle and Driver Information System](#) (NEVDIS) is operated by Austroads Ltd on behalf of driver licencing authorities. It does not store or transmit facial images.

The other system is called the National Driver Licence Facial Recognition Solution (NDLFRS). We host NDLFRS on behalf of states and territories and it will help make driver licences from around the country available via the FVS and the FIS.

Not all jurisdictions have provided information for the NDLFRS. As at **August 2022**, the NDLFRS contains information from Tasmania, Victoria, and South Australia. While this information has been loaded, it is not yet available through the Services. When you apply for a new driver licence or renew your driver licence, your local driver licencing authority will tell you how your information is being shared with us. The Department of Home Affairs will host a replicated copy of your driver licence or proof of age card information in the NDLFRS.

Information in the NDLFRS includes:

- biographic information, such as name, address, date of birth, and gender;
- driver licence information (including learner permits), including licence number and licence type;
- proof of age card information, including card number (South Australia only);
- facial images, and
- biometric templates.

Information held in the NDLFRS remains under state and territory control and can only be shared with the person's consent or where permitted by law.

The NDLFRS does not collect any of the following information: racial or ethnic origin, sexual orientation or practices, criminal record, including traffic infringements or demerit points. However information could be inferred from collected personal information. For example, a person's race might be inferred from an image of their face.

Consent

In most circumstances, your consent is needed before an organisation can use the Services to verify your identity or identify you. If you do not give your consent, the organisation may use a different method to verify your identity which might be slower or less secure.

Driver licence information is collected and held in the NDLFRS in accordance with the Privacy Act. States and territories are permitted by their laws to share your personal information with us, if reasonably necessary, without your consent.

The Department may also disclose your personal information without your consent to law enforcement or security agencies under certain circumstances, if it is required or authorised by law.

How your information is disclosed

We can only disclose your personal information for the purpose of providing the Services in accordance with the Privacy Act. We may disclose your information to government agencies via the Services under certain circumstances, such as to:

- conduct investigations of serious criminal offences;
- conduct investigations related to Australia's defence, security, international relations or law enforcement interests;
- protect facilities or personnel;
- investigate missing people or those who are reported as dead;
- identify people who pose significant risks to public health or safety;
- identify people as part of disaster events or major events; and
- perform security or criminal background checking.

Who can access your personal information

An organisation's use of the Services must be reasonable, necessary and proportionate to its functions or activities, and comply with all privacy and other relevant laws.

In Australia, only approved government agencies and businesses can use the Services. Businesses cannot request a match against a facial image.

Under limited circumstances as authorized by the law, national security, law enforcement and anti-corruption agencies can use the FIS to identify unknown persons without consent. These agencies include:

- the Department of Home Affairs (including the Australian Border Force);
- the Department of Foreign Affairs and Trade;
- the Australian Commission for Law Enforcement Integrity;
- the Australian Crime Commission;
- the Australian Federal Police;
- a police force of a state or territory;
- state and territory crime commissions; and
- state and territory anti-corruption commissions.

The only overseas organisations that can use Services are approved organisations in New Zealand. They cannot request a match against facial images. They can only get a yes or no response to a match request, which means your personal information is not shared. This is provided as part of a reciprocal arrangement that lets Australian organisations use the New Zealand Government's Confirmation Service.

Notification

If your information is collected for the NDLFRS we take reasonable steps to tell you about the collection of your personal information and how it is used.

If a State and territory agency collects your information, it has an obligation to tell you that your information may be shared with us.

The best source of publicly available information on the Identity Matching Service is at www.idmatch.gov.au. It has information for both individuals and organisations.

Correction of your personal information

Agencies are required to take reasonable steps to correct your personal information to ensure that they are accurate, up-to-date, complete, relevant and not misleading.

Since we can't view or modify any information, including information held in the NDLFRS, only data holding agencies that issued your identity document can correct any inaccuracies.

Contact information for each data holding agency is set out on pages 7 to 10.

How your personal information is protected

The Services comply with relevant privacy and other laws including:

- *Freedom of Information Act 1982* (Cth);
- Australian Privacy Principles (APP) under the Privacy Act;
- other state and territory legislation, and
- *Privacy Act 1993* (NZ).

We understand the critical importance of protecting your information from cyber-attacks and data breaches, so we use best practice security and access arrangements. All systems comply with:

- the Australian Government Protective Security Manual; and
- the Australian Government Information Security Manual.

In addition, the FVS and the FIS uses encryption and authorisation procedures approved by the Australian Signals Directorate to ensure data protection, security and confidentiality.

These systems have undergone an independent security review as part of the Information Security Registered Assessors Program (IRAP) certification process, which is the best-practice Commonwealth information security assessment.

Accuracy of facial biometrics

We are committed to using facial recognition technology that is as accurate as possible. We consistently improve it by working with national and international biometric testing bodies.

In the case of requests for identification of an unknown person, our facial recognition technology does not make a confirmed identification. Instead, it assists trained facial examiners in identifying individuals more quickly and accurately by providing them with a shortlist of potential matches for review. This protects against the possibility of false matches.

Need help with a failed match?

In rare cases, your valid proof of identity information may fail to match with the original record. This might be because:

- your personal details were entered incorrectly;
- the original record is incorrect; or
- the system was unavailable.

You can contact the organisation performing the check because it can:

- talk to you about your identity verification options;
- ask us to do a secondary check; or
- ask the issuer to check the quality of their data record.

We cannot look up your personal information, unless it is in a visa or citizenship records.

If you still need help, email the IDMS team at IDMS.manager@homeaffairs.gov.au

If you believe your personal information has been mishandled

If you believe the Services has wrongly collected or handled your personal information, you can email our IDMS team directly at IDMS.manager@homeaffairs.gov.au.

If you need to see or correct your visa, ImmiCard or citizenship information, you can:

- telephone the Global Feedback Unit on 133 177 during business hours,
- complete a request for access form online at: <https://www.homeaffairs.gov.au/access-and-accountability/our-commitments/privacy>, or
- write to:
Global Feedback Unit
Department of Home Affairs
GPO Box 241
Melbourne VIC 3001
Australia.

The Department of Home Affairs' [privacy policy](#) contains further information about how you can complain about a breach of the Privacy Act and how we handle your complaint.

If your information is managed by another agency

If your enquiry relates to another agency's handling of your personal information, we may refer you to that agency. You can also contact that agency directly.

Agencies responsible for personal information used in the Services are:

Passport information

Department	Address and Phone	Online
Department of Foreign Affairs and Trade	RG Casey Building John McEwen Crescent Barton ACT 0021 (02) 6261 1111	privacy@dfat.gov.au

Centrelink and Medicare information

Department	Address and Phone	Online
Services Australia	DHS Complaints and Feedback Reply Paid 7800 Canberra BC ACT 2610 1800 132 468	https://www.humanservices.gov.au/individuals/contact-us/complaints-and-feedback

Driver licence information

State or Territory Department	Address and Phone	Online
NSW – Roads and Maritime Services	Locked Bag 928 North Sydney NSW 2059 (02) 8202 3768	privacy@rms.nsw.gov.au
Victoria – VicRoads	Level 5, 60 Denmark St Kew Vic 3101 13 11 71	https://www.vicroads.vic.gov.au/contact-us/feedback-and-enquiries
Queensland – Department of Transport and Main Roads	GPO Box 1549 Brisbane Qld 4001 (07) 3066 7108	https://www.tmr.qld.gov.au/Help/Privacy.aspx
Western Australia – Department of Transport	P.O. Box R1290 Perth WA 6844 13 11 56	https://www.wa.gov.au/privacy#footer-feedback-form
South Australia – Department of Planning, Transport and Infrastructure	GPO Box 1533 Adelaide SA 5001 1300 872 677	https://www.dpti.sa.gov.au/contact_us/compliments_and_complaints

Tasmania – Department of State Growth	GPO Box 536, Hobart, TAS 7001 1300 135 513	dlu@stategrowth.tas.gov.au
ACT – Access Canberra	GPO Box 158 Canberra ACT 2601 13 22 81	https://www.accesscanberra.act.gov.au/app/forms/accesscanberra_complaint
Northern Territory – Department of Infrastructure, Planning and Logistics	GPO Box 1154 Darwin NT 0801 (08) 8999 1800	https://dipl.nt.gov.au/contact/feedback

Births, deaths, marriages and change of name certificate information

State or Territory Department	Address and Phone	Online
NSW Registry of Births, Deaths & Marriages	GPO Box 30 Sydney NSW 2001 13 77 88	bdm-webmail@justice.nsw.gov.au
Births, Deaths and Marriages Victoria	GPO Box 4332 Melbourne VIC 3001 1300 369 367	https://www.bdm.vic.gov.au/contact-us
Registry of Births, Deaths and Marriages Queensland	PO Box 15188 City East QLD 4002 13 74 68	bdm-mail@justice.qld.gov.au
Births, Deaths and Marriages South Australia	GPO Box 1351 Adelaide SA 5001 13 18 82	dvs.bdm@sa.gov.au
WA Registry of Births, Deaths and Marriages	1300 305 021	bdm@justice.wa.gov.au
Tasmanian Births, Deaths and Marriages	1300 135 513	bdm@justice.tas.gov.au
Access Canberra – Births, Deaths and Marriages	13 22 81	bdm@act.gov.au
Northern Territory Births, Deaths and Marriages	(08) 8999 6119	agd.registrargeneral@nt.gov.au

Contacting Commonwealth and state and territory oversight bodies.

If you believe we or another Commonwealth agency has not provided a satisfactory response to your question or complaint about handling of your personal information, you can contact the Office of the Australian Information Commissioner (OAIC). They can investigate the handling of your personal information, order compensation, and require agencies to change the way your personal information is handled.

The OAIC can receive privacy complaints through:

- the online Privacy Complaint form (refer to the OAIC's website at: <https://www.oaic.gov.au/>);
- by mail at
Office of the Australian Information Commissioner
GPO Box 5218
Sydney NSW 2001;
- by fax at 02 9284 9666; and
- by email at enquiries@oaic.gov.au.

If you believe that a state or territory government agency has mishandled your personal information and you are not satisfied with the response, you may also complain to a relevant oversight agency in that state or territory.

State or Territory Privacy Commission	Phone	Online
Information and Privacy Commission NSW	1800 472 679	ipcinfo@ipc.nsw.gov.au
Office of the Victorian Information Commissioner	1300 006 842	enquiries@ovic.vic.gov.au
Office of the Information Commissioner Queensland	(07) 3234 7373 or 1800 642 753	enquiries@oic.qld.gov.au
WA Information Commissioner	(08) 6551 7888	info@foi.wa.gov.au
Ombudsman South Australia	(08) 8226 8699	ombudsman@ombudsman.sa.gov.au
Ombudsman Tasmania	1800 001 170	ombudsman@ombudsman.tas.gov.au
Office of the Information Commissioner Northern Territory	(08) 8999 1500	infocomm@nt.gov.au