



OFFICIAL: Sensitive

Biometric Collection and Exchange

This factsheet provides information about the Department of Home Affairs' biometrics collection and exchange arrangements.

Biometrics Collection

The Department uses biometrics for identity verification and confirmation of an applicant's identity for any visa application requiring biometrics. In most cases, if an applicant has had biometrics collected for the purposes of one visa application, and subsequently makes an application for a different visa, they will be required to provide biometrics for the purposes of that visa application.

The collection program underpins the Department's international data sharing obligations and maintains the integrity and security of the traveller and migration programs. Data sharing with international partners is an essential and mainstream element of global migration and border management processes.

Offshore collection

The Department's Offshore Biometric Collection Program (OBCP) commenced collecting fingerprints and facial images from visa applicants in December 2010 with an initial target of 17 countries managed by 10 offshore posts. s. 47E(d)

Currently, the Department collects biometrics (fingerprints and facial images) from applicants in 53 countries across a range of visa products, as a requirement of their visa application.

Onshore collection

The Department collects biometrics from a broad range of persons seeking access to Australia's borders including illegal Foreign Fishers in immigration detention; citizenship applicants s. 47E(d) unlawful non-citizens in immigration detention onshore; onshore permanent protection visa applicants; onshore visitor visa renewal applicants and travellers using SmartGates s. 47E(d)

Further information: s. 47E(d)

When are biometrics required?

Visa applicants must provide their biometrics (facial image and fingerprints) if they apply from a country, or for a visa, that is part of the Department's Biometric Collection Program. Further information about the participating countries and visas is available on the Department's website.

OFFICIAL: Sensitive

How we collect biometrics?

Biometrics (or personal identifiers) collected under the Program are digital facial images and 10-digit fingerprint scans obtained using a digital fingerprint scanner. The process is quick, discreet and non-intrusive.

The Department has contracted Australian Biometrics Collection Centres (ABCCs) to provide biometric collection services. ABCCs charge a service fee to the visa applicant for the collection of biometrics.

Visa applicants in participating countries, who are required to provide biometrics, are sent a biometrics request letter shortly after lodgement of their visa application. Applicants who receive a letter must attend an ABCC in person and provide their biometrics.

How do we store biometrics?

The Department stores applicant facial images and fingerprints in a Departmental database which can only be accessed by authorised officers.

The Department retains and uses biometrics collected offshore in subsequent visa applications. That is, visa applicants whose initial application was granted offshore but who later apply onshore to renew their visa may be required to provide biometrics.

Exclusions, Exemptions and Waivers

Further information about the policy waivers, exclusions and exemptions is in the S. 47E(d)

Exchange

Who do we share our data with?

S. 47E(d)

What is checked against M5 partners?

The M5 network involves automated exchange of fingerprint data via the Secure Real Time Platform (SRTP) with three of the partners (NZ, CAN, and the US), while the UK operates manually via the Secure File Sharing Service (SFSS) and is S. 47E(d).

Confirmed matches are recorded in Departmental systems S. 47E(d)

S. 47E(d)

M5 information is protected by strict administrative, technical, and physical safeguards appropriate to the sensitivity of the information. Privacy measures are articulated and given effect in bilateral treaties, arrangements and annexes. The SRTP completed a Privacy Impact Assessment prior to commencement.

Legislative and policy framework for biometric collection and exchange

The Department collects, retains, uses and discloses personal identifiers under the following legislative and policy frameworks and procedural instructions with further information at **Attachment A**.

Attachment A

Legislation

Legislation underpinning the biometric collection and exchange program includes:

For collection:

- Migration Act s257A – person may be required to provide personal identifiers
- Privacy Act APP 3 – collection of solicited personal information
- Privacy Act APP5 – notification of the collection of personal information
- Form 1442i – Privacy Notice ([1442i - Privacy notice \(homeaffairs.gov.au\)](#))
- Form 1243i – Your personal identifiers ([1243i - Your personal identifiers \(homeaffairs.gov.au\)](#))

Further information on the historical and current legislative basis is at 3.1 of the IIB-1486.

For exchange:

- Migration Act s336E – disclosing identifying information
- Migration Act s336F – authorising disclosure of identifying information to foreign countries etc.
- Privacy Act APP6 – use and disclosure of personal information
- Privacy Act APP8 – cross-border disclosure of personal information
- Form 1442i – Privacy Notice ([1442i - Privacy notice \(homeaffairs.gov.au\)](#))
- Form 1243i – Your personal identifiers ([1243i - Your personal identifiers \(homeaffairs.gov.au\)](#))
- Bilateral arrangements are realised under either under a Treaty (for all connections with the US) or a Memorandum of Understanding/Arrangement (MOU/MOA) (for all connections to which the US is not a party). These information-sharing arrangements are designed to meet policy, privacy and legal conditions for international data exchange.
 - These data sharing arrangements are future proofed, high-level documents and cover data exchange for all immigration purposes.
 - The Secure Real Time Platform has a Privacy Impact Assessment.

Definitions:

- Migration Act Section 5A – meaning of personal identifier
- Privacy Act Section 6(1) – meaning of sensitive information and personal information

Policies, procedures and standard operating procedures

The Department's approach to identity and biometrics complies with existing policies and frameworks including:

S. 47E(d)

- List of relevant Policy Statements, Procedural Instructions (PIs) and Standard Operating Procedures (SOPs):

s. 47E(d)

Policy
Statement

IIB-6798

Identity

s. 47E(d)

Released by Department of Home Affairs
under the Freedom of Information Act 1982



OFFICIAL: Sensitive

Biometric Collection and Exchange

This factsheet provides information about the Department of Home Affairs' biometrics collection and exchange arrangements.

Collecting biometrics (facial images and/or fingerprints) from visa applicants is a critical step in anchoring identity to improve security and safety for travellers and the Australian community. Biometric collection improves the integrity of Australia's visa program, reduces identity fraud, and reduces forum and visa shopping.

s. 47E(d)

s. 47E(d)

s. 47E(d)

The Biometric Collection and Exchange programs operate under the authority of the *Migration Act 1958* and its *Regulations*, *Citizenship Act 1948* and its *Regulations*, and the *Australian Border Force Act 2015*. The *Privacy Act 1988* governs how personal identifiers and information are managed, and the *Freedom of Information Act 1982* provides clients with right of access to the personal information we collect and exchange.

Biometrics Collection

The Department uses biometrics for identity verification and confirmation of an applicant's identity for any visa application requiring biometrics. In most cases, if an applicant has had biometrics collected for the purposes of one visa application, and subsequently makes an application for a different visa, they may be required to provide biometrics for the purposes of that visa application.

The collection program underpins the Department's international data sharing obligations and maintains the integrity and security of the traveller and migration programs. Data sharing with international partners is an essential and mainstream element of global migration and border management processes.

Offshore collection

The Department's Offshore Biometric Collection Program (OBCP) commenced collecting fingerprints and facial images from visa applicants in December 2010 with an initial target of 17 countries managed by 10 offshore posts.

s. 47E(d)

Currently, the Department collects biometrics (fingerprints and facial images) from applicants in 53 countries across a range of visa products, as a requirement for their visa application. Further information about these countries and visas is available on the [Department's website](#).

OFFICIAL: Sensitive

s. 47E(d)

The collection of biometrics offshore enables cost effective risk mitigation of threats well before they reach our shores, s. 47E(d)

Onshore collection

The Department collects biometrics from a broad range of persons seeking access to Australia's borders including:

- illegal Foreign Fishers in immigration detention
- citizenship applicants s. 47E(d)
- unlawful non-citizens in immigration detention onshore
- onshore permanent protection visa applicants – s40 of the *Migration Act 1958* ('the Migration Act') mandates the collection of biometrics from onshore permanent protection visa applicants. Temporary visa applicants are not required to provide biometrics
- onshore visitor visa renewal applicants – clients who initially entered Australia through the visitor visa program and who subsequently apply to renew their visa onshore may be required to provide biometrics.
- travellers using SmartGates s. 47E(d)

Further information: s. 47E(d)

When are biometrics required?

Visa applicants must provide their biometrics (facial image and fingerprints) if they apply from a country, or for a visa, that is part of the Department's Biometric Collection Program.

Further information about the participating countries and visas is available on the [Department's](#) website.

How we collect biometrics?

Biometrics (or personal identifiers) collected under the Program are digital facial images and 10-digit fingerprint scans obtained using a digital fingerprint scanner. The process is quick, discreet and non-intrusive.

The Department has contracted Australian Biometrics Collection Centres (ABCCs) to provide biometric collection services. ABCCs charge a service fee to the visa applicant for the collection of biometrics. The Australian Government manages this fee and it is benchmarked against Australia's other international partners and in line with equitable international standards.

Visa applicants in participating countries, who are required to provide biometrics, are sent a biometrics request letter shortly after lodgement of their visa application. Applicants who receive a letter must attend an ABCC in person and provide their biometrics.

How do we store biometrics?

The Department stores applicant facial images and fingerprints in a Departmental database which can only be accessed by authorised officers.

The Department retains and uses biometrics collected offshore in subsequent visa applications. That is, visa applicants whose initial application was granted offshore but who later apply onshore to renew their visa may be required to provide biometrics.

Under the *Archives Act* 1983, the Department is permitted to retain biometrics and the Department's Record Authority 2018/00083401, specifies retention of fingerprint biometrics for 75 years from the date of collection.

Exclusions and Exemptions

Policy Exclusions

S. 47E(d)

Policy Exemptions

S. 47E(d)

S. 47E(d)

s. 47E(d)

Exchange

Who do we share our data with?

S. 47E(d)

What is checked against M5 partners?

The Department has been verifying identity through exchanging biometric data with Australia's M5 partners since 2009. S. 47E(d)

The M5 network involves automated exchange of fingerprint data via Secure Real Time Platform (SRTP) with three of the partners (NZ, CAN, and the US), while the UK operates manually via the Secure File Sharing Service (SFSS) S. 47E(d)

Confirmed matches are recorded in Departmental systems S. 47E(d)

S. 47E(d)

M5 information is protected by strict administrative, technical, and physical safeguards that is appropriate to the sensitivity of the information. Privacy measures are articulated and given effect in bilateral treaties, arrangements and annexes. The SRTP completed a Privacy Impact Assessment prior to commencement.

Legislative and policy framework for biometric collection and exchange

The Department collects, retains, uses and discloses personal identifiers under the following legislative and policy frameworks and procedural instructions with further information at **Attachment A**.

Attachment A

Legislation

Legislation underpinning the biometric collection and exchange program includes:

For collection:

- Migration Act s257A – person may be required to provide personal identifiers
- Privacy Act APP 3 – collection of solicited personal information
- Privacy Act APP5 – notification of the collection of personal information
- Form 1442i – Privacy Notice ([1442i - Privacy notice \(homeaffairs.gov.au\)](#))
- Form 1243i – Your personal identifiers ([1243i - Your personal identifiers \(homeaffairs.gov.au\)](#))

Further information on the historical and current legislative basis is at 3.1 of the IIB-1486.

For exchange:

- Migration Act s336E – disclosing identifying information
- Migration Act s336F – authorising disclosure of identifying information to foreign countries etc.
- Privacy Act APP6 – use and disclosure of personal information
- Privacy Act APP8 – cross-border disclosure of personal information
- Form 1442i – Privacy Notice ([1442i - Privacy notice \(homeaffairs.gov.au\)](#))
- Form 1243i – Your personal identifiers ([1243i - Your personal identifiers \(homeaffairs.gov.au\)](#))
- Bilateral arrangements are realised under either under a Treaty (for all connections with the US) or a Memorandum of Understanding/Arrangement (MOU/MOA) (for all connections to which the US is not a party). These information-sharing arrangements are designed to meet policy, privacy and legal conditions for international data exchange.
 - These data sharing arrangements are future proofed, high-level documents and cover data exchange for all immigration purposes.
 - The Secure Real Time Platform has a Privacy Impact Assessment.

Definitions:

- Migration Act Section 5A – meaning of personal identifier
- Privacy Act Section 6(1) – meaning of sensitive information and personal information

Policies, procedures and standard operating procedures

The Department's approach to identity and biometrics complies with existing policies and frameworks including:

S. 47E(d)

- List of relevant Policy Statements, Procedural Instructions (PIs) and Standard Operating Procedures (SOPs):

s. 47E(d)

Policy
Statement

IIB-6798

Identity

s. 47E(d)

Released by Department of Home Affairs
under the Freedom of Information Act 1982