

INDIGENOUS BUSINESS AUSTRALIA PRIVACY POLICY



1. Purpose of this policy

The purpose of this privacy policy is to clearly explain how Indigenous Business Australia (IBA) handles your personal information, and to let you know about the sorts of personal information we collect and hold.

2. What this policy deals with

IBA is legally bound by the *Privacy Act 1988* (Cth) (**Privacy Act**). There are now 13 Australian Privacy Principles (**APPs**) within the Privacy Act that set out your rights with respect to privacy.

The Privacy Act legislates the way in which IBA collects, stores, provides access to, amends, uses and discloses an individual's personal and sensitive information.

This privacy policy will help explain your rights and IBA's obligations under the Privacy Act.

Credit Information Policy

IBA is a credit provider for the purposes of the Privacy Act. The Privacy Act places strict limitations on IBA's right to collect an individual's credit information. IBA will only collect information about a customer's credit history with their consent and in strict accordance with its obligations under the Privacy Act. IBA has a separate policy that deals with how IBA collects, holds, uses and discloses credit information. IBA's Credit Information Policy can be found at www.iba.gov.au.

3. What is privacy?

IBA will often require individuals to provide certain personal and sensitive information so that we can provide them with particular products and services as a customer or manage their employment with IBA.

The Privacy Act does not regulate a corporation's information. It only regulates information relating to individuals.

As an individual you have a right to know:

- when your personal and sensitive information is being collected by IBA;
- who will have access to this information;
- what the information will be used for; and
- whether it will be disclosed to someone other than IBA.



4. What certain terms in this policy mean

4.1 Personal and sensitive information

Personal information means information or an opinion about an identified individual, or an individual who is reasonably identifiable:

- (a) whether the information or opinion is true or not; and
- (b) whether the information or opinion is recorded in a material form or not.

Sensitive information is a subset of personal information, and includes information or an opinion about a person's:

- Racial or ethnic origin;
- Political opinions;
- Political associations;
- Religious beliefs or affiliations;
- Philosophical beliefs;
- Memberships of professional or trade associations or trade unions;
- Sexual preferences or practices;
- Criminal record;
- Health information;
- Genetic information that is not otherwise health information;
- Biometric information for use in automated biometric identification; and
- Biometric templates.

Sensitive information that IBA has about you is subject to extra protection under the Privacy Act.

5. Why IBA collects, holds, uses and discloses personal information

5.1 Purpose

IBA is required to collect personal information and some sensitive information in order to comply with its obligations under the *Aboriginal and Torres Strait Islander Act 2005* (Cth) (**ATSI Act**) and as a credit provider and as an employer.

IBA is not allowed to obtain personal or sensitive information from you that is unnecessary or not required to fulfil its purposes under the ATSI Act (or any other applicable laws and regulations). IBA will only collect personal information about you if it is reasonably necessary for IBA's functions or is directly connected to IBA's functions or its management of you if you are an employee of IBA.

IBA will not collect sensitive information about you without your consent unless that collection is permitted under the Privacy Act.

5.2 Types of information

The types of personal information IBA collects depends on if you are a member of the public/a customer or a related individual or an employee. The information that IBA tends to collect and handle includes:

Members of the public/customers/related to customers	Employee of IBA
<ul style="list-style-type: none"> • your name; • your gender; • your contact details, including address, email address and phone numbers; • your date of birth; • your marital or relationship status; • your driver's licence number or passport number (or other identification number); • your employment details; • your business details; • your financial details, including your assets, income and expenditure, your dependents, your banking information; • information about your credit history, including credit limit amounts, repayment information, information about defaults, credit worthiness and credit standing; • credit capacity and serious credit infringements¹; • information about your visits to our website or other websites maintained by us or use of our mobile applications – including your server address, your top level domain name (for example .com, .gov, .au, .edu etc), the date and time of your visit to the site, the pages accessed and documents downloaded, the previous site visited and the type of browser used, and if accessing our website through a mobile device, mobile device identifiers (such as the device type, IP address and the operating system); • details of your interactions with us; • your racial or ethnic origin, your criminal history; • any affiliation to a professional or trade association or union; and • sensitive health information in certain circumstances, for example, where you have made a financial hardship request to us due to health reasons or where you receive a payment or income supplement due to a disability or medical condition 	<ul style="list-style-type: none"> • your job application, supporting documents including your name, contact details, resumes, security checks and references • documents produced by employment or recruitment agencies; • your image; • written tasks undertaken during the selection process; • notes from the selection committee during the selection process; • your employment contract and other records relating to your terms and conditions of employment; • details of financial and other personal interests supplied by you and immediate family members for the purpose of managing perceived or potential conflicts of interest (including directorships and shareholdings in entities) • proof of citizenship or residency status; • details of cessation of previous employment; • certified copies of academic qualifications; • records relating to your salary, benefits and leave; • medical certificates or health related information supplied by you or your medical practitioner; • your media (including social media) profile; • your next of kin/emergency contact and their contact details; • taxation details (including your tax file number); • superannuation fund and contributions • information relating to your training and development and performance; • complaint or disciplinary information; • criminal history records; • any membership of a professional trade or association or trade union; and • health records.

5.3 Uses

IBA has several purposes and functions under the ATSI Act. These purposes and functions broadly involve assisting and enhancing the economic interests of Aboriginal and Torres Strait Islander people. We collect, use and disclose your information in the course of performing our functions, including for the following purposes:

¹ IBA has a separate *Credit Information Policy* that provides more information about how IBA deals with credit information. That policy is available at www.iba.gov.au.

- contacting you;
- confirming your identity;
- confirming your eligibility for IBA's products and services (including confirming whether you are an Aboriginal person or Torres Strait Islander or your Australian citizenship or residency status);
- obtaining, exchanging or verifying information about you with credit reporting bodies;
- assessing your application for a product or service and any future request for financial hardship assistance or support;
- managing, administering, reviewing, pricing and providing our products and services (including to you);
- managing our relationship with you, including contacting you and investigating and responding to complaints and handling any disputes with you;
- debt recovery;
- minimising risks and identifying or investigating fraud and other illegal activities;
- complying with any reporting obligations to the Commonwealth or the relevant Minister;
- designing or improving our products and services, our service to you and your experience with us (including conducting or participating in internal and external audits, and collecting and analysis of research data);
- to aid in IBA's compliance with relevant laws and regulations (such as anti-money laundering and counter-terrorism financing laws and taxation laws) or court orders;
- complying with disclosure requirements under any law binding on IBA; and
- managing our relationship with you as an employee.

5.4 Disclosures

We may share your information with third parties for the reasons outlined above or where the law otherwise requires or allows. These third parties can include:

- Australian government bodies;
- your current or previous employers;
- credit reporting bodies and other credit providers (such as banks, credit unions, and financiers);
- guarantors, or potential guarantors, for your IBA product or service;
- credit enhancer, funder or other party acting in connection with funding credit by means of securitisation;
- any party involved in securitising your facility, including the Reserve Bank of Australia, ratings agency, re-insurers and underwriters, loan servicers, trust managers, trustees and security trustees;
- operators of deposit schemes and grants you have or intend applying for, such as the National Housing Finance and Investment Corporation and State or Territory Revenue Offices;
- recognised external dispute resolution and complaint bodies including the Office of the Australian Information Commissioner, Commonwealth Ombudsman and Australian Human Rights Commission;
- other IBA related entities and their associated entities;
- our business partners and consultants;
- joint borrowers;
- our business partners and our service providers (including debt collection agencies, digital banking providers, payment service or card scheme operators, digital hosting and signing platforms and contractors who provide website, IT, marketing, administration, research and other services to support IBA);
- our professional advisers (for example lawyers and consultants), auditors, valuers and insurers;
- organisations involved in surveying or registering a security property or otherwise have an interest in such property;

- organisations involved in a re-organisation or transfer of IBA assets or business;
- any entity to whom we are required or authorised by law to disclose your personal information (for example, law enforcement agencies and government and regulatory bodies including AUSTRAC);
- other entities if IBA forms the view that disclosure is reasonably necessary to conduct our functions and / or to achieve our purpose under the ATSI Act; and
- with your consent – other entities.

The above entities may in turn disclose your personal information to other entities as described in their respective privacy policies or notices.

5.5 Will my personal information be used for direct marketing purposes?

IBA might use customer information (such as your contact details) to provide you with information about other products or services that are related to the products or services that you have with IBA. When you apply for an IBA product or service, IBA will give you the opportunity to opt-out of receiving this marketing information.

If at any time you change your mind about receiving marketing information from us, please email privacy@iba.gov.au or call 1800 107 107.

Under no circumstances will IBA sell or receive payment for licensing or disclosing your personal or sensitive information to third parties.

6. Collection and storage of personal information

6.1 Can you deal with IBA without identifying yourself?

To perform many of its functions, IBA will need to know who you are. For example, if you wish to make an application for a loan, IBA will not be able to process a loan request without you identifying yourself.

However, where IBA can perform its functions without knowing who you are, IBA will give you the opportunity to interact with us anonymously.

6.2 How does IBA collect personal and sensitive information?

IBA may collect personal and sensitive information from you in a number of different ways, including:

- written forms that you complete to obtain products, services or employment from IBA;
- telephone conversations or conversations through audio or video link with you;
- face-to-face interactions with you;
- letter or email correspondence with you;
- webpage or mobile application data collection tools and logs (for example, cookies, JavaScript code and other similar tracking technology); and
- media or social media interactions with you.

IBA may also sometimes collect personal information about you from other sources. IBA will only collect information from other sources if you consent, where we are permitted or required to do so by law (such as under Anti-Money Laundering or Counter-Terrorism Financing laws and taxation laws), or if it is unreasonable and impracticable to obtain that information from you.

We usually collect information about you from the following parties:

- Credit providers such as banks, credit unions or financiers;
- Someone who is, or who is considering being, a guarantor for any product or service we may

provide to you or someone who has, or who is considering, providing security for any product or service we provide to you;

- Credit reporting bodies or debt collection agencies;
- Anyone necessary in order to confirm information about you, including your employment, income and financial history (including Centrelink);
- Our professional advisers, valuers, insurers and service providers (and their contractors);
- Joint borrowers, or any person whom you notify us is acting on your behalf, such as a legal or financial adviser, settlement agent, accountant, executor, trustee, guardian or attorney;
- Digital banking providers, payments systems operators and cards scheme operators.
- Law enforcement agencies or other agencies (or organisations);
- Government agencies, community organisations (including land and sea councils), recognised registers or databases (such as Supply Nation) to confirm your Aboriginality or Torres Strait Islander descent or verify your Australian citizenship or residency status;
- Operators of deposit schemes and grants you have or intend applying for, such as the National Housing Finance and Investment Corporation and State or Territory Revenue Offices.

To perform its functions, IBA will often have to seek financial and credit information about you from third parties. IBA will usually seek your consent to obtain that information².

6.3 How does IBA hold personal and sensitive information?

IBA stores information both manually in paper-based records, and in cloud or other types of networked or electronic systems.

Access to electronic records in IBA's possession and control is protected via appropriate security systems in accordance with the Commonwealth protective security policy.

Where we use cloud infrastructure provided by a third party, to protect your personal information IBA requires:

- that the cloud infrastructure is located in Australia;
- its providers are contractually bound to protect personal information in accordance with the Privacy Act;
- its providers have appropriate security measures in place, including ensuring no unauthorised party is allowed physical or electronic access to the cloud infrastructure

IBA's paper-based records are held in secure offices accessible only by authorised IBA staff and contractors.

IBA will take all reasonable steps to ensure that all files in its possession or control are protected against loss, unauthorised access, misuse, disclosure or modification and that only authorised employees have access to such material.

Personnel files, previous employee files and personal information relating to payroll are archived and stored in appropriate methods in accordance with the Commonwealth protective security policy.

6.4 How long does IBA store personal and sensitive information?

IBA will destroy or de-identify any personal information it receives where:

- IBA did not ask for the personal information to be provided;
- IBA has determined that it could not have collected the personal information; and
- the information is not contained in a Commonwealth record.

² IBA has a separate *Credit Information Policy* that provides more information about how IBA deals with credit information. That policy is available at www.iba.gov.au.

Commonwealth records that contain personal information are managed by IBA in accordance with the *Archives Act 1983* (Cth). Further information regarding how long a Commonwealth record must be kept can be obtained from the [National Archives of Australia](https://www.naa.gov.au).

7. Access to personal and sensitive information held by IBA

IBA will - upon your request and subject to the Privacy Act - provide you with access to your personal and sensitive information that is held by IBA.

To request access to your personal and sensitive information please email privacy@iba.gov.au or call 1800 107 107. IBA will need to verify the identity of anyone who requests access to personal information, to make sure that personal information is not shared with people who have no right to it.

It is important that you provide IBA with clear and appropriate instructions as to the type(s) of personal and sensitive information to which you require access.

IBA will deal with your request to provide access to your personal and sensitive information within a reasonable time period – usually within 30 days of receipt of your request. IBA will not charge you for a request for access to your personal and sensitive information.

7.1 What if IBA does not provide me with access?

There may be some instances where IBA refuses you access to your personal and sensitive information. If this occurs, IBA will provide you with a notice that will set out the reasons for the refusal of access and the mechanism(s) available to you to complain about the refusal (see section 12 below).

For example, IBA may decide not to disclose a record to you that also contains another person's personal information without their consent.

7.2 If the information IBA has is wrong, how do I have it corrected?

It is inevitable that some personal or sensitive information which IBA holds will become out of date. IBA will take reasonable steps to ensure that the personal and sensitive information which is held remains accurate. If you advise IBA of any change to your personal or sensitive information, IBA will amend its records accordingly.

To request a correction to your personal or sensitive information, please email privacy@iba.gov.au or call 1800 107 107.

8. Disclosure of information to overseas recipients

From time to time, IBA may engage service providers located overseas to perform certain of our functions and activities. In the course of providing services to IBA, we may need to disclose your personal information to these service providers. In addition, some service providers may use, hold or store your personal information through a cloud service provider located overseas.

If personal information is sent, used, held or stored overseas, we will take reasonable steps to ensure that our service providers are carefully chosen and have policies, procedures and systems in place to ensure your personal information is otherwise handled in accordance with the Privacy Act.

Where we use cloud infrastructure provided by a third party, to protect your person information, IBA:

- takes contractual measures to ensure its providers do not do anything that would breach an Australian Privacy Principle; and

- requires its providers have appropriate security measures in place, including ensuring no unauthorised party is allowed physical or electronic access to the cloud infrastructure.

9. When using our website

We use cookies and other similar tracking technologies so that we can improve our content and provide you with the best user experience. Cookies are text files which are downloaded to your device when you visit our website and allow our website to recognise your preferences and settings.

In addition, our website and mobile application uses Google Analytics to help us better understand and analyse our website/application traffic and usage. Google Analytics uses cookies which generates information about your use of our website (including your IP address). This information is transmitted to and stored by Google on servers in the United States.

Please note, by using our website, you consent to the processing of data about you by Google in the manner described in *'How Google uses data when you use our partners' sites or apps'* which is located at www.google.com/policies/privacy/partners/ (or any other URL Google may provide from time to time).

You can configure your browser to accept or reject all cookies, including opting-out of Google Analytic cookies at: <https://tools.google.com/dlpage/gaoptout> .

Our website may also use third party social media and video websites (such as, Youtube, Facebook and Twitter). We do not collect or use any information stored in the cookies set by any of those websites. For further information about how they use their cookies, please refer to those third party websites/applications.

10. Notifiable data breaches

IBA must report Notifiable Data Breaches (**NDBs**) to customers and the Office of the Australian Information Commissioner (**OAIC**). A NDB occurs when there is a data breach that is likely to cause serious harm to the persons to whom the information relates. A data breach happens if the personal information held by IBA is lost, or subject to unauthorised access or disclosure.

If a data breach occurs, the Privacy Act requires IBA to make an assessment of whether it is likely to result in serious harm with reference to the following:

- the kind(s) of information;
- the sensitivity of the information;
- whether the information is protected by security measures and the likelihood that any of those security measures could be overcome;
- the persons who have obtained, or could obtain, the information;
- the likelihood of a security technology which renders the information unintelligible to unauthorised persons being circumvented;
- the nature of the harm; and
- any other relevant matters.

At IBA, the response to data breaches is managed by the IBA Privacy Officers. All data breaches must be notified to the IBA Privacy Officers at privacy@iba.gov.au so that the breach can be assessed and managed appropriately.

11. Privacy impact assessments

As required by the *Privacy (Australian Government Agencies – Governance) APP Code 2017*, IBA must prepare a Privacy Impact Assessment (**PIA**) for all high risk privacy projects. A project is a high risk privacy project if IBA considers that the project involves any new or changed ways of handling personal information that are likely to have a significant impact on the privacy of individuals. A register of PIAs conducted from July 2018 is available on the IBA website (www.iba.gov.au).

12. Making a complaint about a breach of the Privacy Act

IBA has a formal complaint management process. This process is applicable to any complaint you may have against IBA in relation to the Privacy Act.

12.1 Submitting a complaint about a breach of the Privacy Act

If you have a concern about the manner in which your personal or sensitive information has been collected, stored, used or disclosed, you may lodge a complaint directly to IBA via telephone, email or the internet:

Telephone: 1800 107 107
 Email: complaints@iba.gov.au
 Internet: <http://www.iba.gov.au/feedback/>

You have the option to remain anonymous, although this may inhibit IBA's ability to investigate your concerns in appropriate detail.

12.2 How would IBA handle such a complaint?

There are a number of stages in the complaint management process. IBA will endeavour to deal with your complaint as quickly as possible – usually within 30 days – and to keep you informed of the progress. If unresolved in the first instance, your complaint will be referred to a complaint officer who is required to be independent and impartial when dealing with the circumstances of your complaint.

12.3 What if you are not satisfied with how the complaint was handled or resolved?

You may make a complaint to the OAIC if you are not satisfied with IBA's response to your complaint regarding a breach of the Privacy Act. For further information about how to make a privacy complaint to the OAIC, please visit the website [Privacy complaints - Home \(oaic.gov.au\)](http://www.oaic.gov.au/privacy-complaints)

13. How will IBA update this policy?

IBA will review this policy periodically to ensure that it continues to provide transparent and current information about how IBA's policies and practices affect your personal and sensitive information.

This policy was last updated 25 July 2024.