

PRIVACY POLICY

POLICY

AUSTRALIAN PRIVACY ACT

General

Under the Privacy Act 1988, Entities have an ongoing obligation to take reasonable steps to handle personal information in accordance with Australian Privacy Principles (APP). This includes protection from misuse, interference and loss and from unauthorised access, modification or disclosure. The Privacy Act also regulates the handling of personal information by the Australian government, ACT Government and the private sector.

An Australian Credit Licensee or Australian Credit Representative will handle an individual or entities personal information with Credit Providers (CP) and Credit Reporting Bodies (CRB). This must be done via adoption of various codes and practices.

Australian Privacy Principles (APP)

Organisations must have an APP Privacy Policy that contains specified info including personal info it collects & how an individual may complain about a breach of the APP's. It must also confirm whether information will be provided to overseas recipients. Policy must be available free of charge and in appropriate format

Tax File Numbers

An organisation must not use or disclose a Government related identifier of which a Tax File number is. This is considered unauthorised disclosure of an individual's private information. Privacy Act offences are penalised under Chapter 2 of the Criminal Code.

Privacy Consent

As an Australian Credit Licensee or Australian Authorised Credit Representative, you must provide acknowledgment of the above requirements via your Privacy Consent.

Direct Marketing

An organisation may only use or disclose personal information for direct marketing purposes in a discrete privacy principal. This allows for use or disclosure of information where the individual has consented for their personal information being used for direct marketing or has a reasonable expectation that their personal information for this purpose and conditions relating to opt out mechanisms are met.

Notifiable Data Breach Reporting Scheme

As a mortgage broker you need to know what is considered as a data breach. There are 3 main criteria:

- ◆ Unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information, that a business holds;
- ◆ This unauthorised access or unauthorised disclosure is likely to result in serious harm to 1 or more individuals, and;
- ◆ The business has not been able to prevent the likely risk of serious harm with remedial action.

A breach is also considered something that may result in serious harm to any of the individuals to whom the information relates. Examples include:

A device (such as mobile phone, tablet or laptop) containing clients' personal information is lost/stolen. A database containing personal information is hacked.

Personal information is mistakenly provided to the wrong person.

If a data breach occurs that impacts a customers' personal information which you access or store, please follow the steps set out in the Notifiable Data Breach Response summary above to ensure you meet the OAIC's requirements. (See Information / Data Breach Policy and Procedure within this guide for more information)

The Office of the Australian Information Commissioner (OAIC) explains the entire scheme on their website. outsource encourage you to make yourself familiar with the document. The website is - www.oaic.gov.au

What you must do:

- Privacy Consent to be presented to client with signed copy returned and held on client file.
- All copies of documents with Tax File Numbers to be fully erased before being placed on client file.
- Client must indicate their preference for Direct Marketing on Privacy Consent which must be noted by the Mortgage Broker with relative digital and written material indicators observed.
- If a breach occurs, you must follow steps set out in the Notifiable Data Breach Response summary and ensure you meet the OAIC's requirements.

The Privacy Consent Statement template is available in ioutsource and a template is available under the "Compliance Templates" tab of the secure Member website. Usage of the Privacy Consent Statement is also clearly described in our Compliance Guide and in the Consumer Lending Compliance Handbook.

Refer to section 15 of the Consumer Lending Compliance Handbook for further information on Privacy.

Websites and Email Signatures

You are required to have a privacy and policy statement on your website and email signature. If you do not already have your own version, you will find templates available on the outsource Member website in the Compliance Templates tab.

The Mortgage Brokers Privacy Policy or a link to how a client can access their Privacy Policy should be visible on a Credit Representatives website, their email signature / disclaimer and other required business documents. Refer to the Advertising Guidelines for additional information as to where the Privacy Policy is required.

Privacy Policy example templates are shown below:

PRIVACY POLICY TEMPLATES

Short Form Privacy Statement

Instructions for use – Customise this statement and incorporate it into your email signature, FBC, Letter of Engagement or your first correspondence with any person about whom you collect personal information.

Privacy - At <insert full name of your organisation>, we are committed to protecting your privacy. We use the information you provide to advise about and assist with your finance needs. We only provide your information to the companies with whom you choose to deal (and their representatives). We do not trade, rent or sell your information.

If you don't provide us with full information, we can't properly advise you. You can check the information we hold about you at any time.

For more information about our Privacy Policy, ask us for a copy <or visit our website>.

The information contained in this email communication may be confidential. If you have received this email in error, please notify the sender by return email, delete this email and destroy any copy.

LONG FORM PRIVACY STATEMENT / PRIVACY POLICY

Instructions for use – Use on Websites, other required business documentation and have available to give to any client who asks for more information about your privacy policy.

Privacy Policy

At <insert full name of your organisation>, we are committed to protecting your privacy in accordance with the Privacy Act 1998 (Cth). This Privacy Policy describes our current policies and practices in relation to the handling and use of personal information.

What information do we collect and how do we use it?

When we arrange finance on your behalf, we ask you for the information we need to advise you about your finance needs and your borrowing capacity. We provide any information that the lenders to whom we apply on your behalf require to enable them to decide whether to lend to you and on what terms.

We also use your information to enable us to manage your ongoing requirements, e.g. refinancing, and our relationship with you, e.g. invoicing, client surveys etc. We may do so by mail or electronically unless you tell us that you do not wish to receive electronic communications.

We may occasionally notify you about new services and special offers, events or articles we think will be of interest to you. We may send you regular updates by email or by post on finance matters. If you would rather not receive this information, please email or write to us.

We may also use your information internally to help us improve our services and help resolve any problems.

What if you don't provide some information to us?

We can only fully advise you about your borrowing capacity and the suitability of a loan if we have all relevant information.

How do we hold and protect your information?

We strive to maintain the reliability, accuracy, completeness and currency of the personal information we hold and to protect its privacy and security. We keep personal information only for as long as is reasonably necessary for the purpose for which it was collected or to comply with any applicable legal or ethical reporting or document retention requirements

We hold the information we collect from you <insert brief details of how and where you store your clients' information>.

We ensure that your information is safe by <insert brief details of how you protect that information, i.e. describe your security measures and procedures>.

This information may be held by us in electronic form on our secure servers and may also be held in paper form. We may use cloud storage or other types of networked or electronic storage to store the information we hold about you. As electronic or networked storage can be accessed from various countries via an internet connection, it is not always practicable to know in which country your information may be held. If your information is stored in this way, disclosures may occur in countries other than those listed.

Overseas organisations may be required to disclose information we share with them under a foreign law. We are not responsible for such disclosure.

Disclosure of personal information overseas

We may hold or process your information on servers located overseas for filtering, hosting or storage purposes, reporting and analytical purposes and for system development testing purposes. If we do this, we make sure that such organisations have the appropriate data handling and security arrangements in place to ensure compliance with this Privacy Policy. While these entities are subject to confidentiality or privacy obligations, they may not always follow the particular requirements of Australian privacy laws.

Where your information is sent overseas it is likely to be to one of the following countries:

- ◆ United States
- ◆ Singapore
- ◆ Serbia
- ◆ Philippines

Will we disclose the information we collect to anyone?

We do not sell, trade, or rent your personal information to others.

We may need to provide your information to contractors who supply services to us, e.g. to handle mailings on our behalf or to other companies in the event of a corporate sale, merger, reorganisation, dissolution or similar event. However, we will do our best to ensure that they protect your information in the same way that we do.

We may provide your information to others if we are required to do so by law or under some unusual other circumstances which the Privacy Act permits.

How can you check, update or change the information we are holding?

Upon receipt of your written request and enough information to allow us to identify the information, we will disclose to you the personal information we hold about you. We will also correct, amend or delete any personal information that we agree is inaccurate.

If you wish to access or correct your personal information, please write to <insert name and/or title of Privacy Officer and address of intermediary>.

We do not charge for receiving a request for access to personal information or for complying with a correction request.

< Describe here the amount or basis on which you will charge for providing access to personal information, if any. If you do not propose to charge for this, insert "We do not charge for providing access to personal information".>

Your consent

By asking us to assist with your finance needs, you consent to the collection and use of the information you have provided to us for the purposes described above.

Dealing with Breaches

We will deal with Breaches in an appropriate and timely manner. There may be internal and external actions that need to be taken. In taking any action, we will be guided by these steps as suggested by the OAIC on responding to a Breach (whether it is actual or suspected):

- Step 1: Contain the Breach and do a preliminary assessment
- Step 2: Evaluate the risks associated with the Breach
- Step 3: Notification
- Step 4: Prevent future Breaches

A copy of the OAIC's "Data Breach Notification - a guide to handling personal information security breaches" can be accessed at <https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/handling-personal-information/guide-to-securing-personal-information>.

Tell us what you think

We welcome your questions and comments about privacy. If you have any concerns or complaints, please contact <insert name and/or title, telephone and email of Privacy Officer>