



State Bank of India

Australia

Privacy Policy

State Bank of India
Australia Branch
May 2019

Contents

About this Privacy Policy.....	2
Our commitment to privacy	2
Privacy laws	2
Collection and use	2
Sensitive information	4
Cookies	4
Disclosure	5
Tax file number and other government identifiers	6
Consent.....	6
Marketing and privacy	6
Accuracy of personal information	7
Requests for details about your personal information	7
Storage	8
Destruction of personal information	8
Complaints	8
Need more information?	9

Please note

Handling of personal information relating to employees is outside the scope of the *Privacy Act 1988* (Cth) if the handling of the information relates directly to a current or former employment relationship between an employee and the State Bank of India.

About this Privacy Policy

This Privacy Policy sets out how the State Bank of India Australia ('we', 'our', or 'us') protects your privacy.

This Privacy Policy also provides you with information about your privacy rights and how we collect, hold, use and disclose personal information.

Our commitment to privacy

As a Global banking and financial services organisation, the State Bank of India has a long history of handling personal information with transparency and openness.

Protecting the privacy and confidentiality of your personal information is fundamental to the way we do business. Our systems are designed to protect your privacy whenever we collect, hold, use or disclose your personal information.

We encourage any person who has a comment, query or complaint about a privacy matter to get in touch with our CEO, Relations or Privacy Officer using the following details:

State Bank of India, Australia Branch
Sydney Office:
Level 31, 264 George Street
Sydney NSW 2000
Phone: (02) 9241 5643
Fax: (02) 9241 0536
Email: info@sbisyd.com.au

Privacy laws

Our aim is to comply with all applicable privacy laws, including the requirements of the Australian Privacy Principles (**APPs**) set out under the *Privacy Act 1988* (Cth) including in the unlikely event of a data breach, due to control failures or due to the actions or inactions of individuals in our employ, through agreement or through third-party contractor arrangements, we will notify you in accordance with the Notifiable Data Breaches (NDB) scheme under Part IIIC of the Privacy Act 1988. We will also take any actions possible to work with relevant authorities in: recovering any physical information that has been taken; or mitigating the risks associated with the breach, to the extent that the breach has exposed or revealed your private information.

Collection and use

We generally only collect and use information necessary to provide our banking and financial products and services to you. We may also collect and use personal information for other reasons where the law allows or requires it.

Most commonly, we will collect and use your information to:

- confirm your identity
- consider your eligibility for products and services
- process your application and provide you with products and services
- contact you about a product or service being provided to you
- comply with any legal or regulatory obligations, or
- perform necessary business functions (such as audits, reporting, planning, and research).

We will tell you how we intend to use your personal information when we collect it. This information will usually be set out in documents provided to you, such as in our application form or our terms and conditions.

We will usually collect personal information directly from you. Most commonly, this will be when you contact us, open an account, fill in an application form, visit our web sites, use our mobile apps, or visit us in person.

If you do not provide us with the necessary personal information, we may not be able to provide you with our products and services.

The type of personal information we collect may include:

- information about your identity (including your name, date of birth, gender, marital status and address)
- contact details (including your phone number and email address)
- your tax file number or tax residency status, and
- financial details (including your annual income, transaction history, and credit history).

We may also be required by law to collect and use personal information. For example, we may be legally required to:

- update our register of members
- verify your identity, or

- assess your capacity to repay a loan.

We have obligations under the *Australian Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (AML Obligations) which require us to carry out client identification and verification procedures. This law requires us to collect and keep records which include your personal information and credit details for 7 years from the date of the last relevant service offered by us.

Collecting information from third parties about you

We may also collect personal information about you from a third party. We will take reasonable steps to let you know when we do this. Our AML obligations permit the use and disclosure of certain personal information held by a credit reporting body (**CRB**) to us for the purpose of verifying your identity under the AML/CTF Act.

From time to time we may receive information about you which did not intentionally collect. If the information is not publicly available or on a Commonwealth record, we will:

- destroy or de-identify the information, and
- comply with any privacy obligations in treating the information.

Sensitive information

‘Sensitive information’ is a type of personal information. Many different types of information can be classified as sensitive information. Among other things, sensitive information includes information or an opinion about a person’s racial or ethnic origins, politics, religious beliefs or health.

We do not generally collect sensitive information about you. We will only collect sensitive information with your express consent or if we are legally required to do so. Our AML obligations require us to collect 'sensitive information' in the *Privacy Act 1988* which may include information or an opinion about your political opinions or membership of a political association to determine if you are a politically exposed person (PEP).

Cookies

A ‘cookie’ is a small text file stored on your computer, mobile or other electronic device. As you browse a website, cookies gather and store some information about your use of the website.

We collect cookies on our website to improve the services we provide and enhance your experience when using the website. Cookies are useful because they allow our website to recognise your device and whether you have visited the website before.

The cookies we collect vary depending on which part of our website you visit and what you are trying to do. Some types of cookies are essential to how our website works and ensure you can access our website in your browser.

Most browsers are set up to accept cookies. You can adjust the settings on your browser to change this. The 'help' function on your browser will tell you how to change your settings. However, if you restrict cookies this may affect your experience when using our website.

Our website might also keep a record that you have visited the website by logging your IP address. An IP address is a numeric label specific to your device. Logging your IP address helps us collect useful information about the ways you use our website.

Disclosure

We may disclose your personal information to third parties in certain circumstances. These include when we:

- deal with third party contractors
- need to disclose personal information to an overseas third party
- share personal information within the State Bank of India, or
- are required to disclose personal information under an Australian law or an order of a court or tribunal.

Dealing with third party contractors

We may need to disclose your personal information to a third party contractor in order to provide our services to you. This is only done on the basis that the contractor will not use your personal information for other purposes.

Third parties may include:

- organisations who do work for us (including marketing, mailing, and IT support work)
- other banks or financial institutions
- auditors, insurers and re-insurers
- organisations we use in funding arrangements (including agents, advisers and researchers), and
- government bodies and law enforcement agencies.

Overseas third parties

In some situations we may need to disclose personal information to an overseas third party.

We will only disclose your personal information to an overseas third party if:

- the disclosure is necessary to undertake a transaction on your behalf, or
- we have your consent and are fully satisfied that the disclosure is in accordance with our privacy obligations at law.

For example, where an overseas transaction is being made, we may need to disclose your personal information to our legal advisers located outside of Australia.

The countries to which we receive and disclose information from include: India, Singapore, United Kingdom, Hong Kong and the European Union. This list of countries may be updated from time to time.

We understand that overseas third parties may not be subject to the same privacy obligations as us. If we disclose personal information to an overseas third party, we make sure there are arrangements in place to protect your personal information.

Sharing information within the State Bank of India

We may also disclose your personal information by sharing information with other branches of the State Bank of India located outside Australia. This may be necessary depending on the product or services which you have applied for. We will obtain your consent to share any personal information with other branches of the State Bank of India.

Tax file numbers and other government identifiers

We may ask you for your tax file number (TFN) when dealing with you. In certain circumstances because of our AML obligations you may not be able to provide a different government identifier, such as a pension number or Medicare number.

We will not use your any identifier as an account, policy or application number. We only use and disclose these identifiers as required or authorised by law. For example, we may be required to disclose your TFN to the Australian Taxation Office or AUSTRAC.

Consent

We will seek your consent to collect, use or disclose personal information about you wherever possible.

Your consent can be express or implied, verbal or written. For example, our loan applications may expressly ask for your consent to a credit reference check.

You may be taken to give implied consent by your actions or inactions. For example, our telephone banking service notifies you that the call may be monitored or recorded for quality assurance purposes. If you choose to continue the call after hearing the notification, you have given us your implied consent to monitor or record the call.

Marketing and privacy

We do not disclose names and addresses to third parties for marketing purposes. However, as providing the best service possible to our customers is fundamental to our business, we may use personal information to identify products and services that may benefit you. We may also contact you from time to time to tell you about new or existing products or services. These communications may be sent in various forms, including by letter, SMS, email or other electronic means.

You can opt out if you do not want to receive marketing information from us.

Accuracy of personal information

Having accurate information about you allows us to provide you with the best possible service. We will take reasonable steps to ensure that your personal information is correct, complete and up-to-date.

Please contact us if you learn that current personal information we hold about you is incorrect, incomplete or out-of-date. We will promptly update our records.

If we disagree with a request you make to correct personal information, you have the right to request that a statement is attached to the personal information setting out your view about why the information is inaccurate.

Requests for personal information

You can find out what personal information we hold about you by making a request. Requests should be made to our Privacy Officer using the details set out on page 1 of this Privacy Policy.

We will not charge you any fee for providing information to you. However, we will need to verify your identity before providing you any information.

We will normally be able to deal with your request immediately. If the request is complex, we will ask you to complete a personal information request form. We can usually deal with even a complex request within 30 days.

We may not be able to tell you what personal information we hold about you in certain circumstances. This includes where:

- the privacy of other individuals is threatened
- the information may be relevant to legal proceedings

- the information would reveal commercially sensitive information, or
- the law prevents us from disclosing the information.

If we are unable to tell you what personal information we hold about you, we will tell you why and try to find other ways to let you access your information.

Storage

Your personal information may be stored in hardcopy documents or electronically in our systems. We use all reasonable methods to protect any personal information that we hold about you from misuse and loss.

We take a number of steps to prevent unauthorised access or disclosure of your personal information. We maintain physical security over our paper and electronic data stores and premises. We also have strong computer and network security.

Destruction of personal information

We will use all reasonable endeavors to destroy personal information if it is no longer needed for:

- the purposes for which we collected it, or
- meeting legal requirements.

We use secure methods to dispose of any hardcopy documents containing personal information. Information stored in electronic form is simply deleted from our systems.

Complaints

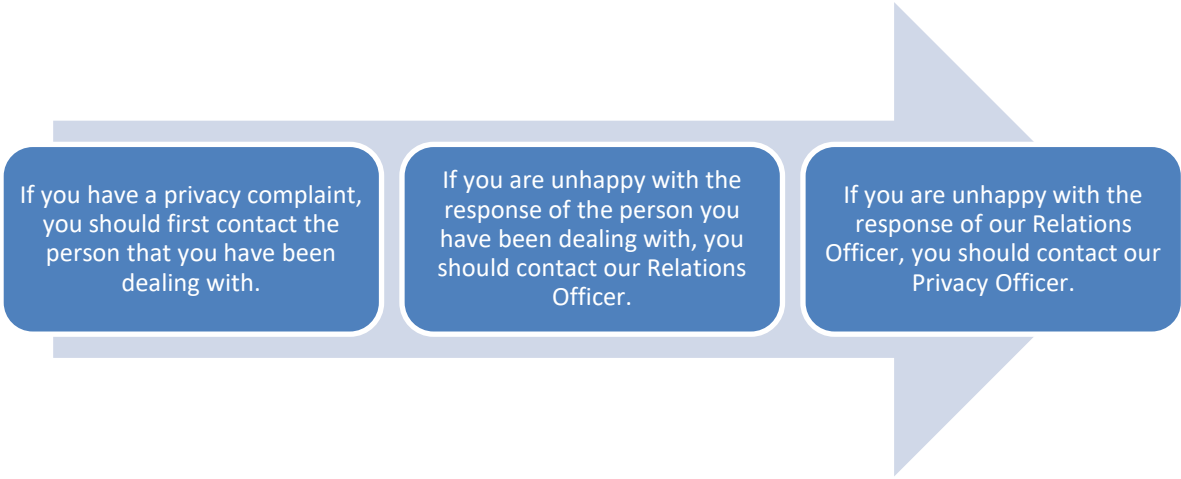
You are entitled to complain if you believe that we have not handled your personal information the right way.

We will acknowledge receipt of a complaint as soon as possible and let you know who is responsible for managing your complaint. We will also try to complete the investigation within 30 days and inform you of the outcome.

If we are unable to resolve the dispute within 30 days, we will:

- tell you the reason or reasons for the delay
- give you monthly updates on the investigation
- work with you to try and agree on a reasonable alternative time frame, and
- tell you when it is expected that a decision will be reached.

Our complaints process is as follows:



If you have a privacy complaint, you should first contact the person that you have been dealing with.

If you are unhappy with the response of the person you have been dealing with, you should contact our Relations Officer.

If you are unhappy with the response of our Relations Officer, you should contact our Privacy Officer.

The CEO, Relations Officer or Privacy Officer can be contacted using the details set out on page 1 of this Privacy Policy.

Need more information?

You should contact the person, department or branch that you normally deal with if you would like more information about this Privacy Policy. You will need to do this between 9.00am and 5.00pm (EST) and Monday to Friday.

Appendix 1 – Credit Policy

When you make a credit application either as an individual on your own behalf or as a director or an agent acting on behalf of an applicant or provide documents as a guarantor, your certified identification documents are reviewed as part of our AML Obligations (coming from the AML/CTF Act). Information required by us may include:

- certified proof of and verification of your identity
- occupation and business activities
- photo ID
- tax returns and tax assessment
- source of Funds
- beneficial owners
- type or the amount of existing credit you had or have, or
- if you have committed a fraud or other serious credit infringement.

To determine your overall credit score and your ability to manage credit, we may exchange credit information and credit reports with credit reporting bodies, other financial institutions, our other agents or other State Bank of India branches.

If you fail to provide adequate information to verify the credit details we will not be able to assess your application.

The credit reporting agencies we or our agents or other State Bank of India branches may use to obtain your credit information are Equifax Pty Ltd, Illion Australia Pty Ltd, Dun & Bradstreet Pty Ltd and Experian Information Solutions Inc. You can download a copy of their privacy policies from their websites. They also have a legal responsibility and obligations under the Privacy Act and our Privacy Policy to keep your information secure.

We use information we obtain from credit reporting bodies, other financial institutions and/or third party agents (Other Entities) to confirm your identity, assess credit applications, manage our relationship with you, assess your skills to manage credit and collect overdue amounts.

We may also share your personal and credit information with Other Entities so they can provide credit reports to others and the Other Entities may include information in reports to assist other credit providers in assessing your credit worthiness.

In accordance with our AML/CTF Obligations and our State Bank of India Record Management Policy we, our agents or other State Bank of India branches must retain your credit information for 7 years from the discharge of your credit facility and may retain records for other business reasons for up to 10 years or a reasonable such time.

Appendix 2 – General Data Protection Regulation

The European Union (EU) General Data Protection Regulation (GDPR) has protections and rights to individuals by harmonizing the data privacy laws of each individual EU country and created more obligations on organisations holding EU located individuals' data. In this Appendix 2 “personal information” means “personal data” in the GDPR.

If you are located in the EU, we are required to provide you with more information about how we collect, hold, use and disclose your personal information as well as being transparent and open about your rights as a “data subject”.

What personal information we collect

Please refer to the main Privacy Policy for details of personal information we collect.

Special categories of personal information

We only will process special categories of personal information about racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union data or biometric data such as fingerprints where you have consented or where we are required to disclose under law.

Keeping of your personal information

We endeavor to keep your personal information for only as long as we need it. Where you cease being a customer we may retain your personal information for legal or regulatory obligations, internal research and analytics or to respond to a question or complaint.

Using your personal information

Please refer to the main Privacy Policy for details of how we use personal information.

Rights as a data subject

As a data subject you have rights on your personal information these may include:

- Right to be informed on you the processing, object or to restrict the processing of your personal information
- Right to access, rectification or erasure of your personal information
- Right to data portability of the information in a format that can be easily reused

In addition to the above you have the right to lodge a complaint and refer to the main Privacy Policy for details or more information and details of the EU jurisdictions where you can find the data protection authorities p<European Commission>.

Where you decline to disclose personal information with us we may not be able to provide you with components of our products and services.

Minors and children’s privacy

Any collection of details of children under 16 will only be with the consent of a parent or guardian.