State Bank of India

Australia

Privacy Policy

State Bank of India
Australia Branch
May 2025

Table of Contents

Purpose....2
Applicability....2
Privacy laws....2
Collection and use....3
Reporting Standards....5
Sensitive information....5
Website....5
Cookies....6
Email....6
Sharing your personal information....6
Disclosure....6
Consent....6
Marketing and privacy....7
Accuracy of personal information....7
Access to personal information....7
Security....8
Workplace surveillance....8
Complaints....9
Changes to the Privacy Policy....10

Purpose

SBIA protects the privacy of all individuals, corporations, entities, whose Personal Information (PI) that the Branch collects and handles.

Adhering to this policy ensures that we manage and govern the PI that is consistent with our obligations under the Privacy law, SBI's group values (Parent / Group) , assist in the prevention of data breach incidents and other privacy concerns so that SBIA (Branch) minimizes the adverse impact and likelihood of such incidents or concerns.

The inadequate management and governance of Personal information may arise from a failure to meet any one of the policy requirements listed below and may result in negative outcome or harm to individuals; a loss of trust in the Branch / Parent's ability to handle and protect personal information, adverse reputational impacts, regulatory action and liability for the Branch / Parent.

The Privacy Act 1988 (Privacy Act) is the principal Australian legislation protecting the handling of personal information about individuals. This includes the collection, use, storage, and disclosure of personal information in both the federal public sector and the private sector. The Privacy Act aims to promote and protect individuals' privacy rights while regulating how Australian Government agencies and organizations handle personal information.

The Office of the Australian Information Commissioner (OAIC) is the independent national regulator for privacy and freedom of information that promotes and upholds individual rights to access government held information and have individual personal information protected.

The Branch and its Parent does not tolerate breaches or interference with Privacy and expects that staff report suspected data breach incidents that involve PI are internally reported within 24 hours of their discovery through the Branch's GRC tool, Parent's Incident Management System (IMS).

The Branch and its Parent expects compliance with the spirit and letter of Privacy Act and that we earn and maintain the trust of our stakeholders, customers, employees by effectively managing and governing PI.

Any request from Regulators will be handled in line with Regulatory engagement policy with the Regulator having unfettered access to the information requested. SBIA will ensure to comply with the regulator's request for an investigation with current (or previous) employees if required.

Applicability

The policy applies to the Branch employees, Contingent workforce, Directors, third parties who handle PI in any record, electronic or material, on our behalf.

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. SBIA will only collect and use an individual's real name as the use of a pseudonym is not in our best interest to do so.

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

- confirm your identity
- consider your eligibility for products and services
- establish your tax status under any Australian or foreign law
- process your application and provide you with products and services
- contact you about a product or service being provided to you
- delivering our products and services
- customer relations including managing our relationship with you,
- responses to market research surveys, competition entries and product development
- assisting with your questions or complaints and/or comply with any legal or regulatory obligations
- perform necessary business functions (such as audits, record keeping, training, reporting, planning, and research)
- developing and testing our technology systems
- collecting overdue payments, or
- or any purpose where you have given consent.

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, driver's license number, passport details 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:

- verify your identity,
- credit information (see section headed credit information below for more details), or
- assess your capacity to repay a loan.

As you interact with us over time, we may collect and hold additional personal information (including but not limited to council rate notices, contracts of sale, etc), use of account, call, email or sms, our website or mobile app, or when we are managing a hardship application or dealing with a complaint or enquiry about your products or services.

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.

In some cases, you might need to give us personal information about other people – such as when you have an authorised representative. In those situations, we are relying on you to tell those people that you are giving us their details, and to let them know about this policy.

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. For example, if you apply for a loan, we might need to ask a credit reporting body for your credit report or conduct a property valuation. We may also collect financial and transaction information from other financial institutions either directly or through you and/or a third-party service provider. We may use information we receive about you, to help us identify and tell you about products and services that may be of interest to you and for administrative purposes.

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. Sometimes, we might collect information about you that's publicly available – for example, from things like social media, telephone directories or public registers, e.g. Australian Securities and Investments Commission (ASIC), Australian Business Register (ABR).

We must also fulfil our legal obligations to Australian and overseas enforcement bodies including Australian Transaction Reports and Analysis Centre (AUSTRAC).

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.

Reporting Standards

SBIA has guidelines in place to ensure reports are submitted in a timely manner and comply with all requirements for creating and submitting payment times reports and keep adequate records of these reports and comply with auditing requirements.

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, nationality, biometric data, (e.g. signature, call recordings), politics, religious beliefs or health information.

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).

SBIA at times may receive unsolicited personal information directly from the customer/entity in which we will ensure to treat this in accordance with the Privacy Act 1988. Unsolicited personal information is personal information that SBIA receives but did not request it, for example, if an individual attaches copies of bank statements to an application form that requests basic financial information, any personal information in the bank statements must be treated as unsolicited, and only the information contained within the form may be handled as personal information.

Website

We use this information to improve and maintain our online channels andt also to improve security, tailor our marketing advertising, tracking, and analysing your session data. Until you log in, or contact us, any browsing you do on our site is completely anonymous.

Here is some of the general information we may collect when you visit any of our online channels or applications:

- the website that referred you to ours
- the browser, operating system or device type you are using
- IP address or device ID
- the date/time and duration of visit
- what you view, and any errors may encounter whilst on our site
- information from third party websites, applications or platforms containing interactive content or that interface with our website and applications, or

- how you navigate through the site and interact with pages (including fields completed in applications).

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.

When you visit our website, we use cookies for security and personalization purposes. 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.

You may change the settings on your browser to reject cookies, however doing so might prevent you from accessing the secured pages of our website.

Email

When we receive emails, we will retain the content of the email and our response to you where we consider it necessary to do so. Your email address will only be used or disclosed for the purpose for which it was provided.

It will not be added to any mailing lists or used for any other purpose without your consent.

Sharing your personal information

There are some situations in which we will share your information with another organization or person, including when you have given consent or at your request. We only share information with third parties that we believe have the proper systems in place to look after your personal information.

Disclosure

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

- deal with third party contractors
- share personal information within the State Bank of India or overseas third-party, aligned with APP 8 and
- are required or authorized by Australian law, by a court or regulatory body. Examples of laws include the Anti Money Laundering and Counter Terrorism Financing Act, the National Consumer Credit Protection Act, and Australia's participation in Automatic Exchange of Information regimes concerning the automatic exchange of financial account information with foreign jurisdictions.

Consent

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

Your consent can be expressed 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 may use your personal information, including your contact details, to provide you with information about products and services, including those of other organizations, which we consider may be of interest to you unless you request not to receive marketing communications.

If you are on the Do Not Call Register while you are our customer, we will infer from our relationship with you that you consent to receiving telemarketing calls from us, unless you notify us that you do not wish to receive such calls.

You can opt out at any time if you do not want to receive marketing information from us by 'unsubscribing' from our email marketing messages, which always include an unsubscribe option. Unless we have first obtained your consent, we will not provide your personal information to other organizations to use for their marketing purposes.

Accuracy of personal information

We take reasonable steps to make sure that the personal information that we collect, use or disclose is accurate, complete and up to date. However, if you believe your information is incorrect, incomplete or not current, you can request that we update this information by contacting us on +61 02 92415643 or via email or by visiting our branches.

Access to personal information

You may request access to the personal information that we hold about you at any time from anyone handling your banking.

We will respond to your request for access within a reasonable time. If we are unable to give you access to any of your personal information, we will explain why we are unable to do so. You can contact us on +61 02 92415643 or via email or by visiting our branches, if you object to the reasons given for not providing you with access.

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, public health or public safety is threatened
- the request for access is frivolous or vexatious
- the information may be relevant to legal proceedings
- the information would reveal commercially sensitive information, or
- the law prevents us from disclosing the information.

In general, there are no fees to access or correct your information, however we may recover a reasonable administration fee for our response to a request for access to personal 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.

Security

Whenever we store your personal information or credit information - we always take proper steps to safeguard and protect it, in accordance with Australian privacy law. We may store your information in hard copy or electronic format. Computer and networks systems are protected using security measures including firewalls and data encryption. SBIA also ensures that employee records are kept separate from non-employee records and has security procedures in place to ensure that the employee records are used or disclosed for purposes that are directly related to the current or former employment relationship.

SBIA is committed to ensuring that staff access to email and internet services is managed in full compliance with applicable Australian laws, including:

- Federal legislation governing the interception of communications over computer networks; and
- Workplace privacy laws applicable in Australia.

There are restrictions on who may access personal information and for what purposes. Our employees, contractors, service providers and authorized agents are obliged to respect the confidentiality of personal information held by us. If we suspect or believe that there has been any unauthorized access to, disclosure of, or loss of, personal information held by us, we will promptly investigate the matter and take appropriate action, and we will comply with any obligations in relation to notifiable data breaches that are in force under the Privacy Act.

Always make sure to keep your personal and login details safe and educate yourself on the best ways to safeguard your information, e.g., protecting your banking details by not sharing your passwords and keeping up to date with any security material we provide to you. We will not ask for your personal or identity details via an email or SMS link. If you receive this type of request, contact us immediately.

When we no longer require your personal information (including when we are no longer required by law to keep records relating to you), we take reasonable steps to ensure that it is destroyed or de-identified. Using or disclosing government-related identifiers (e.g. TFN, Medicare number) are managed in accordance with the records retention policy.

Workplace surveillance

SBIA has the appropriate practices and processes to ensure it complies with workplace surveillance laws. SBIA will ensure to use appropriate surveillance devices and covert surveillance to ensure workplace safety. The Information obtained from covert surveillance will not be used or disclosed other than lawful purpose.

SBIA may conduct Optical surveillance devices, such as cameras and CCTV if the device is clearly visible. In such cases, SBIA will have a sign at each entrance to the workplace telling everyone who enters that they will be under surveillance. SBIA does not operate the use of listening or tracking devices.

Data Breach management

When the Branch or the Third party to which Privacy Act 1988 covers, has reasonable grounds to believe an eligible data breach has occurred, they must notify any individual at risk of serious harm and notify OAIC.

A reportable data breach i.e. eligible data breach occurs when:

- There is unauthorised access to, or disclosure of PI held by the Branch, or Third party.
- PI is lost in circumstances where unauthorised access or disclosure is likely to occur.
- The incident is likely to result in serious harm to any of the individuals to whom the information relates.
- The Branch or third party has been unable to prevent the likely risk of serious harm with remedial action.

In the event of a data breach, the Branch must disclose to OAIC:

- Branch / Third parties name and contact details of the key management personnel.
- Brief description of data breach
- The kinds of information involved.
- Recommendation about the steps individuals should take in response to the data breach.
- Complete the Notifiable Data Breach form as required by OAIC in the prescribed format.
  Notifiable Data Breach Form (business.gov.au)

Complaints

If you have any questions, concerns or complaints about this Privacy Policy, or our handling of your personal information, please contact the privacy officer.

Privacy Officer
Our Privacy Officer's contact details are:
State Bank of India, Sydney,
Mail: 31/264 George St, Sydney NSW 2000
Email: info@sbisyd.com.au
Telephone: +61 2 8042 0500 or +61 2 9241 5643

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 within 24 hours 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.

If you are not satisfied with the outcome of the complaint, then you will be advised to approach AFCA as a free independent means of external dispute resolution or lodge a complaint with OAIC, whose contact details are as follows:

Australian Financial Complaints Authority Limited
G P O Box 3
Melbourne VIC 3001
Tel: 1800 931 678
Fax: (03) 9613 6399
Internet: http://www.afca.org.au/
Email: info@afca.org.au

The Privacy Commissioner
Office of the Australian Information Commissioner
GPO Box 5218
Sydney NSW 2001
Tel: 1300 363 992
Internet: http://oaic.gov.au
Email: enquiries@oaic.gov.au

Changes to the Privacy Policy

The CRCO function is the owner of Privacy policy. The policy is reviewed annually or on any material changes to existing privacy requirements, business plans and practices.