STATE BANK OF INDIA

South Africa

Data Privacy Policy 2023/2024

State Bank of India

South Africa Operations

Data Privacy Policy- 2023 – 2024

Version Number	5
Applicable for Year	2023 – 2024

Document Information

Document Owner	Chief Compliance Officer
Document Prepared By	Chief Compliance Officer South Africa
Document Reviewed By	Compliance/ Risk Committee
Document Approved By	Regional Head Office, Mewana

Contents

DEFINITIONS

No.	Term	Explanation
1.	"Consent"	*means any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information*
2.	"Data Subject"	*means the person to whom personal information relates;*
3.	"De-identify"	*in relation to personal information of a data subject, means to delete any information that—* *(a) identifies the data subject;* *(b) can be used or manipulated by a reasonably foreseeable method to identify the data subject; or* *(c) can be linked by a reasonably foreseeable method to other information that identifies the data subject, and* ***''de-identified''*** *has a corresponding meaning;*
4.	"Electronic communication''	*means any text, voice, sound or image message sent over an electronic communications network which is stored in the network or in the recipient's terminal equipment until it is collected by the recipient*
5.	"Filing system''	*means any structured set of personal information, whether centralised, decentralised or dispersed on a functional or geographical basis, which is accessible according to specific criteria*
6.	"Operator"	*means a person who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party*
7.	"Personal information''	*means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to—* *(a) information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person;* *(b) information relating to the education or the medical, financial, criminal or employment history of the person;* *(c) any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person;* *(d) the biometric information of the person;* *(e) the personal opinions, views or preferences of the person;* *(f) correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;* *(g) the views or opinions of another individual about the person; and*

		(h) the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person;
8.	"Public record''	*means a record that is accessible in the public domain and which is in the possession of or under the control of a public body, whether or not it was created by that public body*
9.	"Processing"	*means any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including—* *(a) the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;* *(b) dissemination by means of transmission, distribution or making available in any other form; or* *(c) merging, linking, as well as restriction, degradation, erasure or destruction of information*
10.	"Record"	*means any recorded information—* *(a) regardless of form or medium, including any of the following:* *(i) Writing on any material;* *(ii) information produced, recorded or stored by means of any tape-recorder, computer equipment, whether hardware or software or both, or other device, and any material subsequently derived from information so produced, recorded or stored;* *(iii) label, marking or other writing that identifies or describes anything of which it forms part, or to which it is attached by any means;* *(iv) book, map, plan, graph or drawing;* *(v) photograph, film, negative, tape or another device in which one or more visual images are embodied so as to be capable, with or without the aid of some other equipment, of being reproduced;* *(b) in the possession or under the control of a responsible party;* *(c) whether or not it was created by a responsible party; and* *(d) regardless of when it came into existence;*
11.	"Responsible party''	*means a public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information*

1. INTRODUCTION

i. The Protection of Personal Information Act (POPIA), is a piece of legislation designed to protect any personal information which is processed by both private and public bodies. Some exceptions exist, but every person who collects, stores and otherwise modifies or uses information is responsible under POPIA and must comply with the conditions required for the lawful processing of personal information.
ii. State Bank of India, South Africa (SBISA) as a financial Institution is also bound by POPIA.
iii. POPIA requires SBISA to inform their clients as to how their personal information is processed and destroyed.
iv. SBISA guarantees its commitment to protecting their client's privacy and ensuring their personal information is used appropriately, transparently, securely and in accordance with applicable laws.
v. This policy sets out how SBISA deals with client's personal information in addition for what purpose said information is used for.
vi. This policy is drafted in conjunction The Protection of Personal Information Act, the Regulations to the POPI Act as well as any other relevant legislation pertaining to data privacy and protection.
vii. This Policy informs our Privacy Notice which is made available to the clients on SBISA website.

2. PERSONAL INFORMATION COLLECTED

i. Section 9 of POPI states that "Personal Information may only be processed if given the purpose for which it is processed, it is adequate, relevant and not excessive."
ii. SBISA collects and processes clients' personal information pertaining to clients' financial needs. The type of information will depend on the need for which it is collected and will be processed for that purpose only. Whenever possible, the bank will inform the client what information they are required to provide and what information is optional. Examples of personal information SBISA collects includes but is not limited to:
    - Clients Identity number/ Passport Number & Visa details, name, surname, address, postal code, marital status, email address, occupation, employer, and how many dependent's they have;
    - Description of client residence, business, assets; financial information and banking details.

iii. The bank has agreements in place with all its Product Suppliers, Insurers and third-party Service Providers to ensure there is a mutual understanding with regard to the protection of our clients' personal information. SBISA's suppliers will be subject to the same regulatory requirements

iv. Personal information must only be collected from the data subject it relates to. Specific attention must be paid to the collection of information from a minor, ensuring consent is obtained from a competent person who is the parent or lawful guardian of the minor.

v. Before collecting personal information, or as soon as reasonably practicable after it is collected, steps must be taken to ensure that the data subject is aware of:
   1) The purpose for which the information is being collected;
   2) Who is collecting the information (i.e. provide the name and address of SBISA);
   3) What information is being collected;
   4) From which source the information is being collected (if not directly from the data subject);
   5) Whether the supply of information is voluntary or mandatory; and
   6) Any intentions to transfer the information to a different jurisdiction or internally within the organisation and the level of protection provided.

3. HOW PERSONAL INFORMATION IS USED

i. A client's personal information will only be used for the purpose for which it was collected and agreed. This may include:
   a) Providing products or services to clients and to carry out the transactions requested;
   b) Conducting credit reference searches or verification;
   c) Confirming, verifying and updating client details;
   d) For the detection and prevention of fraud, crime, money laundering or other malpractice;
   e) Conducting market or customer satisfaction research;
   f) For audit and record keeping purposes;
   g) In connection with legal proceedings;
   h) Providing our services to clients to carry out the services requested and to maintain and constantly improve the relationship;
   i) Providing communications in respect of SBISA and regulatory matters that may affect clients; and
   j) In connection with and to comply with legal and regulatory requirements or when it is otherwise allowed by law.

ii. According to **section 10** of POPIA, personal information may only be processed if certain conditions are met which are listed below:

a) A client consents to the processing — consent is obtained from client during the on-boarding or application and needs analysis stage of the banking relationship;

b) The processing is necessary — in order to conduct an accurate analysis of client's needs for purposes of amongst other credit limits, Anti-money laundering, prevention of tax evasion etc, certain personal information is required by law;
c) Processing complies with an obligation imposed by law on State Bank of India;
d) The Financial Advisory and Intermediary Services Act (''FAIS'') requires Financial Service Provider's (''FSPs'') to conduct a needs analysis and obtain information from clients about their needs in order to provide them with applicable and beneficial products;
e) Processing protects a legitimate interest of the client — it is in the client's best interest to have a full and proper needs analysis performed in order to provide them with an applicable and beneficial product or service, this requires obtaining personal information;
f) Processing is necessary for pursuing the legitimate interests of SBISA or of a third party to whom information is supplied — in order to provide clients with products and or services both the bank as well as its service provides need certain personal information from the clients to make an expert decision on the unique and specific product and or service they require.

iii. Personal information can be used for a secondary purpose only if the information has been de-identified to an extent that it is not possible to re-identify the data subject or consent has been obtained from the data subject to use the personal information for that secondary purpose.

iv. Personal information which is not required for any legal or contractual obligation must be destroyed or de-identified if a data subject withdraws their consent for its use.

4. DISCLOSURE OF PERSONAL INFORMATION

i. The bank may disclose a client's personal information only to a third-party service provider with whom it has agreements in place to ensure that they comply with confidentiality and privacy conditions.
ii. The bank may also disclose client's information where it has a duty or a right to disclose in terms of applicable legislation, the law or where it may be necessary to protect its rights.

5. SAFEGUARDING CLIENTS INFORMATION

i. It is a requirement of POPI to adequately protect the personal information the bank holds and to avoid unauthorised access and use of the personal information. SBISA will continuously review its security controls and processes to ensure that its clients' personal information is secure. The following procedures are in place in order to protect clients' personal information:

a) The information officer is the Chief Operating Officer, whose details are available below and who is responsible for the compliance with the conditions of the lawful processing of personal information and other provisions of POPI. He is assisted by the Chief Compliance Officer who will function as the Deputy Information Officer.

b) This policy is applicable throughout SBISA and training on this policy and the POPI Act takes place as and when required.

c) Each new employee will be required to sign an employment contract containing relevant consent clauses for the use and storage of employee information, or any other action so required, in terms of POPI;

d) Every employee currently employed within SBISA will be required to sign an addendum to their employment contracts containing relevant consent clauses for the use and storage of employee information, or any other action so required, in terms of POPI;

e) SBISA must secure the integrity and confidentiality of the personal information it holds. To achieve this, SBISA must have in place relevant processes, procedures and systems to prevent loss of, damage to, or unauthorised destruction of personal information; and unlawful access to or processing of personal information. This includes applying the privacy impact assessment process.

f) SBISA'S third-party service providers will be required to sign a service level agreement guaranteeing their commitment to the protection of personal information;

g) Where personal information is considered (including where amnesty for removal has been granted by the National Credit Regulator) to be no longer needed for any purpose, SBISA must ensure this information is destroyed or permanently de-identified, if reasonable to do so. Exceptions to this include, but are not limited to, instances where the personal information is required by a particular record retention law, or required for some other lawful purpose.

h) Consent to process client information is obtained from clients (or a person who has been given authorisation from the client to provide the client's personal information) during the introductory/on- boarding stage of the relationship.

ii. SBISA must not transfer personal information about a data subject to a third party who is in a different jurisdiction unless:

a) The third-party recipient is subject to similar laws as South African legislation with regards to the processing of personal information;
b) The data subject consents to the transfer;
c) The transfer is necessary to fulfil the performance of a contract between the data subject and SBISA; or
d) The transfer is for the benefit of the data subject however it was not reasonably practical to obtain the consent of the data subject at the time, but it is likely that the data subject would have given consent.

6. ACCESS AND CORRECTION OF PERSONAL INFORMATION

i. Clients have the right to access the personal information the bank holds about them. Clients also have the right to ask SBISA to update, correct or delete their personal information on reasonable grounds. A client may exercise his/her right to request for the correction or deletion of his/her personal information or request for deletion of record in terms of section 24 (1) of POPI. The client will be required to complete Form 2 in terms of the Regulations of POPI, added as Annexure 1 of this policy.

ii. Once a client objects to the processing of their personal information, SBISA may no longer process said personal information. A client may exercise his/her right to object to the processing of his/her personal information in terms of Section 11(3) of POPI. The client will be required to complete Form 1 in terms of the Regulations of POPI, added as Annexure 2 of this policy.

iii. SBISA will take all reasonable steps to confirm our client's identity before providing details of their personal information or making changes to their personal information.

iv. The details of the Information Officer and head office are as follows:

INFORMATION OFFICER DETAILS

NAME:	Chief Executive Officer
TELEPHONE NUMBER:	011 778 4504
FAX NUMBER:	011 788 6769
POSTAL ADDRESS:	P O Box 2538, Saxonworld, 2132
PHYSICAL ADDRESS:	11 Cradock Avenue, Rosebank, 2196
E-MAIL ADDRESS:	ceo.rsa@statebank.com

DEPUTY INFORMATION OFFICER DETAILS

NAME:	Chief operations Officer
TELEPHONE NUMBER:	011 778 4504
FAX NUMBER:	011 788 6769
POSTAL ADDRESS:	P O Box 2538, Saxonworld, 2132
PHYSICAL ADDRESS:	11 Cradock Avenue, Rosebank, 2196
E-MAIL ADDRESS:	mgrbanking.rsa@statebank.com

HEAD OFFICE DETAILS

TELEPHONE NUMBER:	011 778 4500
FAX NUMBER:	011 788 6769
POSTAL ADDRESS:	P O Box 2538, Saxonworld, 2132
PHYSICAL ADDRESS:	11 Cradock Avenue, Rosebank, 2196
E-MAIL ADDRESS:	mgrbanking.rsa@statebank.com
WEBSITE:	za.statebank

7. DATA QUALITY OF PERSONAL INFORMATION

i. Reasonable steps must be taken to ensure that personal information is complete, accurate, not misleading and updated when necessary. To achieve this, SBISA has in place relevant processes, procedures and systems to ensure personal information is recorded and updated appropriately, including customer-initiated processes.

ii. SBISA must respond promptly to requests from a data subject to correct or update their personal information.

iii. A data subject may request SBISA to correct or delete personal information that is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully. Such requests may be received directly from a credit bureau on behalf of the data subject. When such a request is made, SBISA must inform the data subject once the action has been completed.

9. POTENTIAL OR ACTUAL BREACHES OF OBLIGATIONS

i. For privacy-related breaches, employees must report the breaches as soon as they are aware to VP Systems as well as the Information Officer.

ii. In addition, where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorised person, the Chief Compliance Officer must notify the Information Regulator as soon as he/she becomes aware.

iii. SBISA must also notify the data subject(s) concerned, as soon as it becomes aware, unless the identity of the data subject(s) cannot be established.
iv. Any other incidents must be reported in terms of the Standard Operating Procedure for reporting of Cyber Security/ Information Security Incident.

10. Responsibilities of Employees when dealing with personal information.

It is the responsibility of the employee to:

1. safeguard client's personal information at onboarding, during the client / bank relationship and after the client relationship has ended.
2. Person Information will be collected directly from you when you complete a product application form on paper. The employee will be responsible to keep the form in a safe lockable storage.
3. The employee will ensure that client information is not shared with anyone without client consent.
4. The employee will ensure that they reasonably protect all client's information that they deal with.
5. It is the responsibility of the employee to ensure that they keep a clean desk policy, making sure no client information is kept on the desk unattended

ANNEXURE 1

SOUTH AFRICA
(Reg. No. 1996/18176/10)

Request for Correction or Deletion of Personal Information or Destroying or Deletion of Record of Personal Information

Mark the appropriate box with an "x".
Request for:

☐ Correction or deletion of the personal information about the data subject which is in possession or under the control of the responsible party.

☐ Destroying or deletion of a record of personal information about the data subject which is in possession or under the control of the responsible party and who is no longer authorised to retain the record of information

A	**DETAILS OF THE DATA SUBJECT**
Name(s) and surname / registered name of data subject:	
Unique identifier/ Identity Number:	
Residential, postal or business address:	
Contact number(s):	
Fax number/E-mail address	
B	**DETAILS OF RESPONSIBLE PARTY**
Name(s) and surname / registered name of responsible party:	
Residential, postal or business address:	

Contact number(s):	
Fax number/ E-mail address:	
C	**INFORMATION TO BE CORRECTED/DELETED/DESTROYED**
D	**REASONS FOR *CORRECTION OR DELETION OF THE PERSONAL INFORMATION ABOUT THE DATA SUBJECT IN TERMS OF SECTION 24(1)(a) WHICH IS IN POSSESSION OR UNDER THE CONTROL OF THE RESPONSIBLE PARTY ; and or REASONS FOR *DESTRUCTION OR DELETION OF A RECORD OF PERSONAL INFORMATION ABOUT THE DATA SUBJECT IN TERMS OF SECTION 24(1)(b) WHICH THE RESPONSIBLE PARTY IS NO LONGER AUTHORISED TO RETAIN. (Please provide detailed reasons for the request)**

Signed at _____ this day of _____20___

_____

Signature of data subject/designated person

ANNEXURE 2

SOUTH AFRICA
(Reg. No. 1996/18176/10)

Objection to the Processing of Personal Information or Destroying

A	**DETAILS OF THE DATA SUBJECT**
Name(s) and surname / registered name of data subject:	
Unique identifier/ Identity Number:	
Residential, postal or business address:	
Contact number(s):	
Fax number/E-mail address	
B	**DETAILS OF RESPONSIBLE PARTY**
Name(s) and surname / registered name of responsible party:	
Residential, postal or business address:	
Contact number(s):	
Fax number/ E-mail address:	
C	**REASONS FOR OBJECTION IN TERMS OF SECTION 11(1)(d) to (f) (Please provide detailed reasons for the objection)**

Signed at _____ this day of _____20___

_____

Signature of data subject/designated person

ANNEXURE 3

Privacy Notice

State Bank South Africa treats the personal information of its clients with utmost discretion. The Protection of Personal Information Act (POPIA), 4 of 2013, which aims to give effect to the constitutional right to privacy and promote the fair and transparent use of personal information, further strengthens our resolve, and requires us, to protect our clients' information appropriately.

POPIA defines 'personal information' as any information that can be used to identify you as an individual or a legal entity. Examples of personal information are your identity number, account number, telephone number, email address or physical address. As part of our commitment to protecting your personal information, and in complying with the law, our processing activities involving personal information are aligned with POPIA.

We also process all personal information in line with the Code of Conduct for the banking industry. Following an application from the Banking Association South Africa (BASA), which represents banks (including SBISA), the Information Regulator issued this code in terms of chapter 7 of POPIA. The code outlines and expands on the specific obligations that members of BASA (banks as responsible parties, operators, or joint responsible parties) have when processing their clients' personal information, and does not replace the provisions of POPIA.

Our Privacy Notice sets out how we will use your personal information, and it applies to any information that you give us or that we may collect from third parties.

Please familiarise yourself with the privacy notice properly before sharing your information with us. Once you give your personal information you consent to us processing your personal information.

What personal information is:

Your personal information includes the following:

- ✓ Your gender (as required for statistical purposes or by law).
- ✓ Your marital status, nationality, or social origin.
- ✓ Your age, physical and mental health and well-being, medical conditions, and disability.
- ✓ Your religion, conscience, belief, culture, and language.

- ✓ Your education.
- ✓ Your financial information (like your income and expenses, loan repayments, investments, assets, and financial needs).
- ✓ An identifying number or symbol (like account, identity, or passport numbers).
- ✓ Your email address, physical address, or telephone number.
- ✓ Your location and online identifiers [this can be internet protocol (IP) addresses or geolocations].
- ✓ Your employment history.
- ✓ Your biometric information (like your fingerprints and facial and voice recognition).

There may be circumstances in which we will collect your special personal information. It may include the following:

- ✓ Your race or ethnicity.
- ✓ Your criminal behaviour.

We will collect and process your special personal information only:

- ✓ if we have your consent to do so;
- ✓ if it is necessary to establish, exercise or defend a right or obligation in law;
- ✓ to comply with a law or for historical, statistical or research purposes; or
- ✓ if we are otherwise allowed to do so by law.

Why we collect and process your personal information:

To offer financial products and services to you, we need to collect, use, share and store your personal and financial information to do the following:

- ✓ Verify your identity.
- ✓ Assess the risk of fraud and money laundering.
- ✓ Enter a banker–client or a banker–third-party relationship with you.
- ✓ Contractually engage with you in terms of loans and credit.
- ✓ Understand your financial needs to offer you the best services and products.
- ✓ Develop suitable products and services to meet your needs.
- ✓ Market relevant products and services to you.
- ✓ Do market research and conduct client satisfaction surveys.

- ✓ Search for, update or place your records at credit reference bureaus and government agencies.
- ✓ Assess your ability to receive credit or to give collateral of any kind, including guarantees or suretyships.
- ✓ Offer other related banking and insurance services to you.
- ✓ Record and monitor communication between you and us, and use these recordings to verify your instructions in order to analyse, assess and improve our services to you, as well as for training and quality purposes.
- ✓ Communicate with you about products that may be of interest to you via post, phone, SMS, email, and other electronic media, including social-media platforms, our ATMs, mobile applications, and online banking services.
- ✓ Assess how you use our digital channels so we can offer enhanced services and client experience.

You have the right to refuse to give us your personal information, but your refusal may limit our ability to provide the required financial services to you. We will collect from you only information that is necessary and relevant to the services or products that we offer. And we will collect and use your personal information only if we are lawfully allowed to do so. We may send you direct marketing, but you can unsubscribe at any time by opting out on the relevant internet-based platform or by informing us directly. If we use third-party data providers, we will ensure that they are lawfully allowed to share your information with us.

If we process your information, it will be because:

- ✓ we have your consent to do so;
- ✓ we have an obligation to take actions in terms of a contract with you;
- ✓ we are required by law to do so;
- ✓ doing so will protect your legitimate interest; and/or
- ✓ we or a third party has a legitimate interest to pursue.

Processing children's information We will collect and process the personal information of children only with the consent of a competent person (whether a parent, legal guardian, or other person) or if we are lawfully allowed to do so. In line with the Banks Act, 94 of 1990,

How we collect your personal information We collect your personal information in the following ways:

- ✓ Directly from you when you complete a product application form on paper.
- ✓ Indirectly from you when you interact with us electronically. When you are browsing our website or using our mobile applications, we may collect information from you, like your IP address and server logs.
- ✓ From other sources, for example public databases, data aggregators and third parties (or indirectly through your interactions with third parties), as well as other financial institutions, credit bureaus and fraud prevention agencies.
- ✓ Through agents or third parties who collect information on our behalf.

Whom we share your information with Protecting our interests may sometimes require sharing specific client information with third parties, for example if a payment failed because there was not enough money in an account. Also, if it is required to protect the public interest, we may share information about a client's debt with credit bureaus or debt collection agencies. Entities and third parties we may share your information with the following:

- ✓ Banks and other financial institutions.
- ✓ Regulatory authorities, including the Information Regulator.
- ✓ Industry bodies and ombudsmen.
- ✓ Law firms and auditors.
- ✓ Insurers.
- ✓ The South African Police Service.
- ✓ The South African Fraud Prevention Services.
- ✓ The Payments Association of South Africa.
- ✓ Other third parties (contractually, by law, or for protecting a legitimate interest).

When sharing your information with recipients in other jurisdictions, we will ensure compliance with applicable laws. We will not sell your information to third parties and will market to you only in line with applicable laws and your marketing preferences, using your preferred communication method if it is practicable. How we protect your information We are committed to ensuring that your information is secure. To prevent your information from being accessed or shared without authorisation, we have reasonable physical, electronic, and managerial procedures in place to protect the

information we collect. All online transacting sessions are encrypted, and your personal information is stored in line with internationally accepted banking information security practices. How long we keep your information We will keep your information only for as long as we need it for a lawful business purpose or as required by law and any other statutory obligations. We may keep your personal information for longer than required if you have agreed or if we are lawfully allowed to do so. If we need to keep your personal information for longer than required, and more specifically for historical, statistical or research purposes, we will do so with the appropriate safeguards in place to prevent the records from being used for any other purpose. Depending on regulatory requirements, we may keep your information for varying periods once our relationship with you has ended. When it is not necessary for us to have your information, we will take all reasonable steps to destroy or de-identify it. You have the right to ask us to confirm whether we have any information about you. If we do, you may also request a record of that personal information, as well as information about all third parties with whom we have shared your personal information. Once we have given the information to you, you may ask us to:

- ✓ correct or delete your personal information that we have or control if it is inaccurate, irrelevant, excessive, outdated, incomplete or misleading or has been obtained unlawfully;
- ✓ destroy or delete our record of your personal information that we are no longer authorised to keep in terms of regulatory requirements; or
- ✓ stop or start sending you marketing messages by informing us in writing or through our branch network, call centres or website.

This Privacy Notice explains how SBISA may use cookies and similar technologies on our online banking channels in compliance with the Protection of Personal Information Act (POPIA) in South Africa. By accessing and using our online banking channels, you agree to the practices described in this notice.

What are Cookies and How We may use Them?

Cookies are small text files that are placed on your device (computer, tablet, smartphone, or any other device) when you visit a website. These cookies enable us to recognize your device, collect information about your browsing activities, and enhance your experience on our website. Cookies can also remember your preferences and may help us deliver personalized content and offers.

Authentication and Security Cookies: These cookies are essential for verifying your identity and ensuring the security of your online banking sessions. They help us prevent fraudulent activities and unauthorized access to your accounts.

Types of Cookies We May Use

Preference and Settings Cookies: Preference cookies enable us to remember your preferences, such as language selection and font size, to provide a more personalized and user-friendly experience.

Session Management Cookies: Session cookies are temporary and are used to maintain your session during your online banking activities. They expire once you log out or close your browser.

Analytics and Performance Cookies: We use these cookies to gather information about how you use our online banking channels, which helps us improve their performance and usability.

Your Consent and Managing Cookie Preferences

By using our online banking channels, you consent to the use of cookies as described in this notice. You have the right to manage your cookie preferences. Most web browsers allow you to control cookies through their settings. You can choose to block or delete cookies, but please note that doing so may impact your online banking experience and some functionalities may not work correctly.

Data Sharing and Third Parties

We do not share cookie data from our online banking channels with third parties for marketing purposes without your explicit consent. However, we may use trusted third-party service providers to analyze and improve our online banking services. These providers are bound by confidentiality and data protection agreements.

Security and Retention of Data

We take the security of your personal information seriously. The data collected through cookies on our online banking channels is protected by industry-standard security measures. We retain the cookie data for a duration necessary to fulfill the purposes outlined in this Privacy Notice or as required by law.

Your Rights

As an online banking customer, you have the right to:

- Withdraw your consent to the use of cookies at any time.
- Access the personal data collected through cookies.
- Request correction or deletion of your personal data.

Changes to this Notice

We may update this Privacy Notice from time to time to reflect changes in our practices or for other operational, legal, or regulatory reasons. The updated version will be made available on our online banking platforms, and the date of the latest revision will be indicated at the top of the notice.

If you want to verify the information, we have about you or want us to update, change, or delete it, you can:

- ✓ refer to our Promotion of Access to Information Manual, which is available at za.statebank
- ✓ call the SBISA; or
- ✓ Go to a SBISA branch.

Complaints You can submit complaints about the processing of your personal information by phoning the SBISA ON 100 778 4500 or sending an email to mgrbanking.rsa@statebank.com Or, if you are not satisfied with the way we have dealt with your complaint, you can contact the Information Regulator by completing the prescribed POPIA form 5 and emailing it to POPIAComplaints@inforegulator.org.za. For more information visit the Information Regulator website at https://inforegulator.org.za.

Our contact details the contact details of our Information Officer and Deputy Information Officer are below.

Information Officer Ashutosh Kumar Deputy Information Officer Kirti Kumar Physical address:

The Mall offices

11 Cradock Avenue 3rd Floor.