



Privacy Notice for European Union (EU) NRI Customers

Version 2.0
Issue Date:03/07/2023

Privacy Notice for European Union (EU) NRI Customers

1. Introduction: State Bank of India, (hereinafter referred to as "SBI", "Bank", "us", "our", or "we"), is committed to protect the privacy and security of your data (Personal Data ("PD") / Sensitive Personal Data ("SPD")). Bank shall process data collected from you in compliance & accordance with the EU General Data Protection Regulation (GDPR) 2016 and the provisions of this notice.

General Data Protection Regulation requires that data controller (Bank) provide notice to data subjects (customers), before they collect, process, and use the data. This privacy notice is an approach to fulfil Bank's obligations under EU GDPR.

This privacy notice applies to data, processed by the bank as a controller (or) for the Bank (by third parties/vendors), whether in physical (or) electronic mode. This notice is the Bank's attempt to inform prospective customer/s, what the Bank does with data collected, why & how we process it and what it ultimately means to you.

2. Definitions: The following terms are regularly used in the Privacy Notice:

"Regulation" means the EU General Data Protection Regulation 2016 (EU GDPR) and any laws or regulations implementing it.

"Controller" (or) Data Controller means the natural (or) legal person, public authority, agency or other body which alone or jointly with others, determines the purposes and means of processing Personal Data. In this case, State Bank of India is the controller.

"Personal Data" (PD) means any information relating to an identified or identifiable natural person (data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

"Sensitive Personal Data" (SPD) means a specific set of "special categories" of data that must be treated with extra security, like ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

"Personal data breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to, personal data transmitted, stored or processed. Sharing of data pursuant to order / direction of court / tribunal or regulator in India shall not be construed as 'Personal data breach'.

"Processing" means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

"Processor" means a natural (or) legal person, public authority, agency, or other body which processes PD/SPD on behalf of the controller.

3. Information collected from Customer/s: Bank will collect and process your personal data provided through application forms, mobile apps, devices like ATM, and data collected from public domain like social media, GST portal, face-to-face and electronic communication (including telephone conversations), etc. in order to provide our services to you.

We may collect information about you from others (as mentioned below), and the Bank after ascertaining the genuineness of the same may add it to the Data it already holds and use in the manner described in this Privacy Notice.

If data is collected from Third Party providers to provide relevant marketing, offers, services to you, the same would be used & processed with your consent only. The third-party providers include email service providers, public data bases, social media sites as well as other third parties as deemed appropriate.

If data is collected from Credit Information agencies/companies, risk management and fraud prevention agencies, national & government data bases, the same would be retained & used as deemed legally appropriate.

4. Information from Online Activities: Bank collects information from your internet activity through cookies, which are controlled through internet browsers. While using the bank's website through your digital and electronic devices, the Bank performs various checks designed to ascertain your identity/accuracy/residential status to ensure compliance with regulatory obligations. The checks include identifying the IP address, information about use of website/mobile app, which includes device type, operating system, screen resolution etc.

5. When & how the Bank collects PD/SPD: The Bank collects PD/SPD from its customers/prospective customers:

- i. When you request for & use products/services. Further during your transactions with us.
- ii. When you apply for products, enquire about products (or) engages with us (or) our representative who is involved in the transaction concerning you.
- iii. When you use the Bank's website & online services like mobile application and visit our branch/offices.
- iv. When you email/call/respond to our email/call or during meetings with our bank staff or our service providers/ representatives.
- v. When you provide PD/SPD in writing. The PD/SPD may be on application forms, records of your transactions, etc.
- vi. When you make available information publicly.

6. Information we process about Customers include:

- i. Personal details such as name, address, signatures, date of birth, father's name, mother's name, email address, nationality, marital status, gender, your occupation, education and qualifications, annual income, and source of income and phone numbers.
- ii. Copies of photographs, current overseas residential address and permanent residential address proof, viz. visa, passport, driving license, utility bills, bank statements, national ID cards. PAN card, overseas tax-identification number, and overseas country-specific unique identifiers.
- iii. Transaction details
- iv. Financial information/objectives and experience,
- v. Voice /biometric may also be used for enrolment (or) authentication purposes.
- vi. Details of nominee, witnesses, guardians which includes their addresses and relationship with you.
- vii. CCTV footage and other information obtained through electronic means.
- viii. IP addresses

7. Lawful grounds for processing Personal Information: Bank will process your personal data in compliance with GDPR by relying on one or more of the following lawful grounds:

- i. You have explicitly agreed to our processing for a specific reason.
- ii. Allow us to take required actions to provide product/service and/or to make/receive payments.
- iii. The processing is necessary to perform the agreement we have with you.
- iv. The processing is necessary for compliance with legal obligations under certain laws.
- v. The processing is necessary for the purposes of a legitimate interest pursued by us, which might be:
 - a) to ensure that our customer accounts are well-managed.
 - b) to prevent, detect, investigate, and prosecute fraud and alleged fraud, money laundering and other crimes.
 - c) to protect our business and to comply with laws that apply to us and/or where such processing is a contractual requirement of the services or financing you have requested.
 - d) to provide services to you and protect our business interests.
 - e) to ensure that complaints are investigated.
 - f) to evaluate, develop or improve our services; or
 - g) to keep our customers informed about the relevant services unless you have indicated at any time that you do not wish us to do so.

8. Purposes of collecting and processing your Personal Data:

Bank will use your information for the following reasons:	The Legal basis for processing:
To provide and manage your account/s and provide agreed services	As necessary for performance of our agreement. As required by law. In the legitimate interests of the Bank to ensure that your accounts are well managed so that customers are provided best services and protect our business interests.

To provide requested information & statements about your account/s	As necessary for performance of our agreement As required by law.
To resolve complaints & enquiries.	As necessary for performance of our agreement As required by law. In the legitimate interests of the Bank to ensure that complaints are investigated & resolved in the best interests of customers.
For analysis (including credit/behavior scoring) statistical, historical, product and market research	As permitted by law. In the legitimate interests of the Bank to develop, build, implement and research business models to protect the Bank's business interests.
To evaluate, develop & improve our services	In the legitimate interests of the Bank to continually evaluate, develop and improve our products & services and provide services to you.
To reach out to help by post, phone, text, email, and other digital methods. This may be for: a) managing your accounts. b) meeting our regulatory obligations c) to keep you informed about products and services you hold with us and send you information about products or services (including those of our subsidiaries/JV) which may be of interest to you.	As permitted by law. Where we have agreed to contact you in our agreement. If it's in our legitimate interests to share information with you about products/services that you might be interested. You have the right at any point of time to Opt-out of such mails/calls/messages free of charge in an easy & transparent manner.
For debt collection & related services.	If the same is in our legitimate interests to collect any debts owed to us. As permitted by law.
To comply with RBI, regulatory obligations and reporting duties including to prevent, detect, investigate, and prosecute fraud and alleged fraud, money laundering and other crimes. Bank may record CCTV image as and when you visit the Branch/ATM.	As permitted by law. To prevent fraud & for further investigation as per Legal guidelines. In the legitimate interests of the Bank to prevent and investigate fraud, money laundering and other crimes. The processing is a contractual requirement of the services you had requested.
Assess application/s submitted by you to carry out fraud/Money Laundering/ identity & screening and other mandatory regulatory checks.	If the data is publicly available (or) you made the data public. If the processing is in our legitimate interests or to protect our business interests. As permitted by law.
Monitoring/recording of communications including phone calls to further improve services.	In the legitimate interests of the Bank to validate your instructions given to us, to prevent & detect fraud /other crimes. To analyse, assess & improve bank's offerings, for training purposes, improve customer service standards and protect bank's business interests.
To share information with relevant authorities, including RBI/Income Tax and other government authorities, credit reference agencies, fraud prevention agencies in India and overseas regulators/authorities.	As permitted by law. In the legitimate interest of the Bank in performing certain credit checks to enable make effective business decisions. The Bank has a legitimate interest in assisting Law Enforcement Agency prevent/detect frauds.
To share your information with our partners & service providers. When we ask for your consent, we will provide you with more information on how we will use your data based on your consent.	As necessary for performance of our agreement. In the Bank's legitimate interest in using third party to provide bank's services on our behalf. As permitted by law.

Before processing your personal data, the Bank places robust safeguards to ensure your privacy is protected and prior to collecting your PD/SPD, we ensure that your interests/fundamental rights & freedoms are protected at all costs.

9. Implementation of adequate physical & technical security controls: The Bank is responsible for implementing suitable security measures to protect data against loss or theft as well as unauthorised

access, disclosures, copying, use or modification.

Bank shall adopt/assess/review/update appropriate physical, technical & administrative measures to ensure the security of data, including the prevention of their alteration, damage and loss, unauthorized processing or access having regard to the nature of the data and the risks to which they are exposed by virtue of human action or the physical/ natural environment.

10. Storage of PD/SPD and Data Security: All information you provide to us is stored/saved in a secure manner. Where we have given you (or where you have chosen) a password/pin which enables you to access certain parts of our website/services, you are responsible for keeping such password/pin confidential. We advise you not to share your password/pin with anyone.

In addition, we limit access to your data to those employees, agents, contractors and other third parties on a need-to-know basis. Third parties processing your PD/SPD will only process on our instructions, and they are subject to a duty of confidentiality. We have put in place procedures to deal with any suspected data security breach and will notify you of a suspected breach, where we are legally required to do so.

11. Automated decision making: Bank carries out automated anti-money laundering and sanction checks. The monitoring of your transactions might reveal a money laundering (or) fraud risk to the Bank. This might result in the Bank calling for additional information/details from you. Subsequent to your revert, if the Bank decides that your transactions pose a fraud (or) money laundering risk and/or is inconsistent with your previous submissions, Bank has the right to restrict/block operations in the account (consistent with regulatory guidelines issued).

12. Sharing of Information: To help us provide/ improve services, your data may be processed internally and externally by other third parties. We may use third parties for processing, servicing, monitoring of your data. We may outsource some services to third parties having expertise in performing the required processing activities ensuring no drop in the service standard. However, the data transfers would take place after signing of data transfer agreements incorporating due safeguards. Due to the size and complexity of our operations, it is not possible for us to name each of our data recipients in this notice.

13. Sharing of information outside EU: Information about you in our possession may be transferred to other countries i.e. outside the European Union (including but not limited to India) for any of the purposes described in this Privacy Notice. You understand and accept that these countries may have differing (and potentially less stringent) laws relating to the processing of personal data afforded to the information it holds and that such information can be subject to the laws and disclosure requirements of such countries, including disclosure to governmental bodies, regulatory agencies and private persons, as a result of applicable governmental or regulatory inquiry, court order or other similar process. In addition, a number of countries have agreements with other countries providing for exchange of information for law enforcement, tax and other purposes.

14. Data Retention: We will keep the information in our systems or with third parties for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements. or as required to comply with any legal obligations to which we/you are subject to.

15. Communication: We may communicate with you via letter, telephone, text (or similar) messages, e-mail or other electronic means.

When you contact us through any of our communication channels including visiting a local branch or calling the telephone banking service, we will verify your identity by asking you of questions based on information known to us about you and the transactions on your account. We may record your calls for training, quality, and security purposes.

16. Marketing Information: We and other members of our group may use your information from time to time to inform you by letter, telephone, text (or similar) messages, email or other electronic means, about similar services which may be of interest to you or them. You may opt out of marketing communication at any time.

17. Rights of Data Subjects (DS): You are entitled under the GDPR to the following rights in respect of your personal data:

- i. You may request to access your data provided by you (or) processed by us. This enables you to receive a copy of the personal data we hold about you and to check that we are lawfully processing it.

- ii. You may request to correct/update/amend PD/SPD, particularly if found to be inaccurate. It is important that the personal data we hold about you is accurate and current. Please keep us informed if your personal data changes during your working relationship with us.
- iii. You may request deletion of your PD/SPD, if you think the Bank does not have the right to process it, which would be subject to effective regulatory requirements and Bank's policies/procedures in this regard.
- iv. You can withdraw a given consent at any time, without affecting the lawfulness of earlier processing based on consent before such withdrawal in specific cases.
- v. Be informed about the processing of your personal data (i.e., for what purposes, what types, to which recipients it is disclosed, storage periods, any third-party sources from which it was obtained).
- vi. You have right to object to processing for a particular purpose or to request that we stop using your information when processing is based on necessity (or) for the purposes of legitimate interests pursued by us or third parties including profiling.
After such request objecting to processing your PD/SPD, we shall no longer process the data unless we demonstrate compelling legitimate grounds, like establishment, exercise, or defence of legal claims.
- vii. Request the restriction of processing of your personal information. This enables you to ask us to suspend the processing of personal information about you.

Upon receipt of such a request, Bank shall ensure that the requests are addressed in a timely manner and in compliance with the applicable laws and regulations. If we determine that the request cannot be fulfilled, the bank will respond with a reasonable justification for denial of such request. Further we will inform you, the necessary recourses available. We will maintain records of all such requests and any such statements from you, irrespective of their status of processing.

18. Additional Information: If you exercise any of the aforesaid rights, the Bank will respond within one calendar month. If the bank is unable to respond within one month, due to complexity issues, the Bank may extend this period by a further two calendar months, which will be duly informed to you. If the request is being made electronically, the Bank will provide relevant information electronically, wherever possible. We will provide this information free of charge unless the request is manifestly unfounded or excessive.

19. Right to Complain to the Supervisory authority: You have a right to lodge a complaint with the supervisory authority of state of residence (or) work for data protection issues.

20. Changes to this privacy notice: We reserve the right to update this Privacy Notice at any time. This Privacy Notice is subject to annual review. Any changes made to this Privacy Notice in future will be placed on Bank's website and where appropriate, may be notified to you by email.

21. Disclaimer: The internet is an open system, and the Bank does not guarantee that data, which the registered user furnishes will not be intercepted or accessed by others and decrypted. SBI or its vendors/partners/employees/directors/agents & representatives shall not be liable or responsible, should any confidential or other information provided by you or pertaining to the visitor (including bank account information, passwords, credit/debit card details, transaction details) are intercepted and subsequently misused by an unintended recipient.

SBI is responsible for data only on its own domain and not on the redirected ones.

22. Contact us: Please feel free to contact us through your home branch or through Data Protection Officer (DPO) at gmcompliance.dp@sbi.co.in or through our local representative based at EU at ceo@statebank-frankfurt.com if you have any questions about this Privacy Notice.