# ANTWERP BRANCH

## PRIVACY NOTICE FOR STATE BANK OF INDIA'S CLIENTS, SUPPLIERS AND WEBSITE VISITORS

2023

## 1. About this privacy notice

This privacy notice contains important information on how State Bank of India ("**we**", "**our**") processes personal data from its clients (prospects, existing or former clients), suppliers and website visitors.

State Bank of India focuses mainly on wholesale clients, but we have a small number of retail clients which are mainly employees and former employees of State Bank of India.

This privacy notice therefore applies to:

- Our suppliers and/or business partners;
- Our existing clients, prospects and former clients;
- Physical persons who are legal representatives, directors, shareholders or authorised personnel of our corporate clients; as well as their beneficial owners, trustees, other associates of our corporate clients/suppliers, or persons exercising control over them; and
- Retail clients, being physical persons who wish to receive or receive our products and services for personal, family or household purposes;Third parties whose personal data are provided to us by our clients/suppliers;
- Any other business contacts;
- Visitors of our website be.Statebank.

Together referred to as ("**you**" or "**your**").

In this privacy notice, we explain how we will process your personal data, how we will protect it and how long we will store it. We also explain the rights you have in respect to your personal data. We will store your (personal) data as securely as is reasonably possible and protect it against loss and unauthorised disclosure or access. We will treat your personal data in compliance with the applicable legislation on data protection, including the General Data Protection Regulation (EU Regulation of 27 April 2016), abbreviated as the GDPR.

This privacy notice does not contain information about how and why we use cookies. If you want to know more about our use of cookies, please read our cookie notice on our website be.Statebank.

## 2. Who controls your personal data?

State Bank of India, with registered office in Belgium, B-2018 Antwerp, Hoveniersstraat 29, is the controller of your personal data. We are responsible to process your personal data in accordance with the law.

## 3. What personal data do we collect?

Your personal data is all information relating to you, or on the basis of which you may be identified. Hence, anonymous data, without a possibility to identify you, cannot be considered as personal data.

For the purposes referred to below *(see section 4)*, the following personal data will be processed:

For clients:

- standard personal information (name, first name(s), address, date and place of birth, phone number, e-mail address, etc.);
- financial identification data (bank account number, etc.);
- professional information (such as your function held, representation powers etc.);
- for retail clients: information on your assets and liabilities (loans, mortgages, income, properties etc.);
- Photos/videos (through our surveillance security system when you visit our premises).

For suppliers:

- Identification data (name, surname, title, etc.)
- Contact details (professional e-mail address and phone number);
- Financial data (bank accounts, etc.);
- Professional / Skills and training;
- Any other additional/optional information you give us when we have contact with you (by telephone, by e-mail or at trade fairs or events);
- Photos/videos (through our surveillance security system when you visit our premises).

For web visitors:

When you visit our website, we collect the following information:

- **Device information**. We automatically receive information about the device and software you use to access our website, such as your IP address, your web browser type, operating system version, the nature of the device from which you are visiting the website (e.g., a personal computer or a mobile device), and the identifier for any handheld or mobile device that you may be using.
- **Usage information**. When you use our website, we can collect certain information about your use of the website, including the actions you take on our website and the content, features, and activities that you access in our website via the use of "cookies" (and similar technologies). These small files that store information on your computer's browser enable us to improve your ease of use and offer you relevant services.
  If you would like more information about our use of cookies, please refer to our [Link to the cookie notice].
- **Information provided by you.** You may decide to provide personal data (i.e. account number and IBAN) when you fill in the form on our website (i.e. IBAN Form to calculate your IBAN).

In the context of the whistleblowing, we may process any information provided by the whistleblower to us, or that we have collected during the verification of the reported breaches.

## 4. What is the purpose for processing your personal data?

The primary reason we process your personal data is to manage our contractual relationship and fulfil our legal obligations. Our main purposes thus include,:

For clients:

- compliance with our legal obligations (e.g. FATCA reporting, AML and KYC requirements, external and internal reporting …);
- managing customer relationships (e.g. such as providing you with further information on our services, assisting and answering your requests, evaluating specific conditions under which we can enter into a contract; providing products or services to our corporate clients of whom you are an employee etc.);

  managing our own business arrangements

- preventing and detecting fraud and ensuring security **(**protecting our employees and assets through managing access to our offices and our IT tools etc.)
- ensuring security of property and persons and business continuity (through our surveillance security system when you visit our premises).

  The processing of your data is justified and necessary within the framework of our legitimate interest, and in particular to secure our premises and protect our assets.

  As such, we collect and process the photos/videos taken by our surveillance cameras system when you visit our premises.

- public relations and marketing: we may use your personal data to inform you about our activities, services or newsletters, which we believe may be of interest to you. We will contact you if you explicitly ask us to do so, or if we believe that you may be interested in a service or that a given service could benefit your company/organisation.

For suppliers:

- Managing business relationship with the company that you represent
- Managing our own business arrangements
- Public relations and marketing : we may use your personal data to inform you about our activities, services or newsletters, which we believe may be of interest to you. We will contact you if you explicitly ask us to do so, or if we believe that you may be interested in a service or that a given service could benefit your company/organisation.
- Ensuring security of property and persons and business continuity (through our surveillance security system when you visit our premises)

  The processing of your data is justified and necessary within the framework of our legitimate interest, and in particular to secure our premises and protect our assets.

  As such, we collect and process the photos/videos taken by our surveillance cameras system when you visit our premises.

For web visitors:

- For the proper functioning of our website, on the basis of our legitimate interest in providing you with a functioning website, and
- For the purpose of analysing your browsing behaviour on our website, but only if you have given your prior consent.
- For assisting and answering your requests (i.e. IBAN form).

If you would like more information about our use of cookies, their retention period, etc., please refer to our [Link to the cookie notice].

In the context of whistleblowing, we may process personal data for the handling of disclosures from whistleblowers, i.e. processing and verifying reports of misconduct and taking appropriate action in response to disclosures. For more information regarding the processing of your personal data in the context of whistleblowing, please consult the whistleblower policy and its annexures available on request to the DPO.

More details are provided in the table in Appendix 1.

## 5. What are the legal grounds for processing your personal data?

We can only use your personal data if we have an adequate legal basis to do so. The legal basis that justify the processing of your personal data are as follows:

- it is necessary to perform a contract with our client or to take steps before entering into a contract;
- it is necessary to comply with our legal obligations, e.g. KYC, AML, sanctions screening, whistleblowing, etc.;
- you have consented to the processing of your personal data, e.g. when we take pictures during social events;
- it is in our legitimate business interests e.g. building security if you visit our office, or to protect our IT infrastructure.

## 6. Where does your personal data come from?

Most of the personal data we collect comes directly from you and consists mainly in information you provide in the context of our business relationship, for example :

- you send us information for client admission purposes;
- you send us information so we can verify your representation powers and enter into a contract with our client;
- you apply for our products and services (including when providing us with collateral in relation to such product/services);
- we talk over the phone or meet in person at our office or your office;
- you use our websites.

We may collect data through third parties we work with or use, such as:

- fraud prevention agencies and background information providers, such as Thomson Reuters, Worldcheck, KYC register;

- commercial data and analytics providers (i.e. Dun & Bradstreet);

- your or our client's legal and/or financial advisers, consultants and notaries;

- reporting agencies, brokers, banks; or

- information from publicly available sources (i.e. Belgian Official Gazette, Kruispuntbank voor Ondernemingen, public domain sources) to confirm signatory powers and company's structure.

## 7. What if you do not provide your personal data to us?

If you do not want to give us your personal data and the personal data is necessary for (i) client admission purposes, (ii) provision of products and services, or (iii) provision of further information on our products or services, then we may not be able to enter into a contract or provide the requested services, products or information.

## 8. Who will have access to your personal data?

***Internal use***

The employees of State Bank of India and directors and/or members of our management committees may have access to the personal data, or may receive your personal data for the aforementioned purposes *(see section 4)*. We may also transfer this information to other companies of our group in the framework of these purposes. For example, our headquarters are based in India and may store some information on you or may be involved in providing services to you or assisting us with compliance issues or controlling that we duly comply with our legal requirements (such as KYC, AML). In this respect, we may need to transfer personal data. We enter into EU Model clauses to make sure that your data is safe and not further disclosed. Such contract is available on request.

***External use***

For the purposes mentioned in section 4, personal data may be disclosed and possibly processed by third parties:

- We may disclose your personal data to third parties, external providers as well as contractors and consultants who process personal data for purposes described in this notice. This may include IT platform management or support services, infrastructure and application service providers (Finacle), payment services (SWIFT), security agents, screening agencies (Worldcheck). We ensure that contractual mechanisms are in place to protect your personal data.
- We may also provide your personal data to any EU or Indian competent law enforcement body, tax authorities, courts, judicial, arbitration and mediation instances, financial authorities, regulatory and law enforcement agency, where disclosure is necessary (i) as a matter of applicable law or regulation, or (ii) to exercise, establish or defend our legal rights.

- We may also disclose your personal data with our auditors, accountants advisors, legal representatives and similar agents in connection with the advisory services they provide to us.

The employees, directors, representatives and aforementioned service providers, authorities and administrations must respect the confidential nature of the personal data which they receive and can use this information only in connection with the applicable legal provisions and, where appropriate, our instructions. Further information can be provided upon request.

## 9. Are your personal data transferred outside the European Economic Area or the European Union?

Our group companies and third party contractors and consultants operate around the world. This means that some of the recipients of your personal data may be based in countries outside of the European Economic Area (EEA) and the European Union (UE) whose laws may not provide the same level of data protection. More precisely, we may transfer your personal data to our headquarter in India.

In such cases, we will ensure that there are adequate safeguards in place to protect your personal data that comply with our legal obligations. These adequate safeguard might be a data transfer agreement with the recipient based on standard contractual clauses approved by the European Commission for transfers of personal data to third countries. You are welcome to contact us for more information regarding the adequate safeguards we have in place in relation to such data transfers.

## 10. How long will your personal data be retained?

Your personal data will be stored no longer than is necessary for the purposes mentioned above (*see section 4)*.

Since the need to retain data depends on the type of data and the purpose of the processing, retention periods may vary considerably.
Below are the criteria on which we base our retention periods:

- How long do we need the data to provide the service requested?
- Have we established and announced a specific retention period?
- Have we obtained consent to extend the retention period?
- Are we subject to a legal, contractual or a comparable obligation?

As a general rule, we keep your data to address limitation periods as well as periods prescribes by law and regulations (for instance the AML legislation). These periods mainly amount to 10 years following the end of our contractual relationship.

We also keep images and videos recorded on our surveillance cameras around our premises for 1 month following your visit. This period can be extended upon the request of police authorities / public prosecutor or a judicial service. This will be the case when the images show a (potential) criminal activity or incidents.

Your personal data will be erased after expiry of the abovementioned applicable retention periods.

## 11. What are your rights with regard to the processing of your personal data?

According to the applicable legislation concerning data protection, you have the right to contact us at any time with a request to:

- access your personal data : data subjects may ask to receive more information about personal data or even a copy of the data that are processed about them.

- rectify your personal data: Data subjects have the right to request the deletion or rectification of erroneous, fragmented, inadequate or obsolete personal data.

- erase your personal data (or 'right to be forgotten'): data subjects have the right to obtain the erasure of their personal data in specific circumstances, amongst others if their data is not needed anymore in order to achieve certain purposes.

- restrict or object to the processing and transfer of your personal data means that in certain circumstances, the processing of data may for example be ‘frozen’, and limited to storage of the data, with the exception of any other use.

- receive your data in order to transmit them to another controller (right to data portability): When it is technically feasible, data subjects have the right to ask us to transfer their personal data directly to a third party or to themselves. State Bank of India will assess on a case-by-case basis whether it is technically feasible to comply with the request (in particular depending on the format in which data portability is requested). If it is not possible for State Bank of India to comply with the request, State Bank of India will communicate the reasons for the technical impossibility to the data subject and will offer an alternative to the latter, where possible.

- the right to withdraw your consent at any time if the processing activity is based upon your consent (this will not affect the lawfulness of the processing based on consent before the withdrawal).

- the right to be informed: you have the right to be informed, at the latest at the time of collection of your data, about the processing we carry out, your rights relating to it and the exercise of these rights.

- the right not to be subject to a decision based solely on automated processing, including profiling means that data subjects may require that a natural person is involved in the processing of their personal data. However, we do not take decisions based solely on automated processing.

We may require you to provide verification of your identity to ensure that you have a legitimate right to make the request and to verify that we provide the answer to the person that has the legitimate right to send us one of the abovementioned requests and to obtain the information.

Please note that in certain circumstances as provided by law we may withhold access to your information or that we may not grant your request where we have the right to do so under applicable data protection legislation.

When you exercise your rights, no fee will be charged unless we consider the request to be manifestly unfounded or excessive (this will be the case, for example, when it is a repeated request).

However, we may charge you a reasonable sum not exceeding our reproduction costs for any additional copies requested.

For any request relating to your rights, we will respond to your request within one month. However, this period may be extended to two months if the request proves to be complex and/or because of the number of requests we have to deal with. In the event of an extension of this period, we will inform you of this by giving you the reason for this decision.

You can lodge a complaint with the Data Protection Authority if you believe that State Bank of India did not act in compliance with the legislation on data protection, including the GDPR. "Gegevensbeschermingsautoriteit" – "Autorité de protection des données", Drukpersstraat 35, 1000 Brussel, T: +32 (0)2 274 48 00; F: +32 (0)2 274 48 35; Email: contact@apd-gba.be, Website : www.autoriteprotectiondonnees.be

You can contact our Data Protection Officer (DPO) for more information about these rights as explained in point 14 of this privacy notice.

## 12. How do we protect your personal data?

We protect your personal data against unauthorised access, unlawful use, accidental loss, corruption or destruction.

We use technical measures such as encryption and password protection to protect your data. We also use operational measures to protect the data, for example by limiting the number of people who have access to the databases in which our records are held.

We review our IT policy to keep up to date with current best practice.

## 13. Changes

We may modify the privacy notice included in this start letter from time to time, within the limitations determined in the relevant applicable legislation concerning data protection.

Thus, we suggest you to periodically read this privacy notice, which can also be found on our website www.sbiantwerp.com, in order for you to understand how we process and protect your personal data.

## 14. Questions?

You can contact our Data Protection Officer if you have any question on the above:

- by e-mailing to dposbi@bdo.be
- in writing to :

BDO - DPO SBI Antwerp

The Corporate Village

Da Vincilaan 9 - Box E.6

1930 Zaventem – BELGIUM

* * *

# Appendix 1

| Purposes of the Processing | Nature of Personal Data |
|---|---|
| **Compliance with our legal obligations**<br>**1.** Prevention of money-laundering, the financing of terrorism compliance with sanctions relating to embargoes<br>**2.** Compliance with tax regulations and performance of legal notifications (CRS / FATCA reporting etc.)<br>**3.** Compliance with applicable financial regulation (monitoring reporting risks, monitoring of transactions in accordance with legal patterns, measuring risk scores, prevention of market abuse etc.)<br>**4.** Monitoring of beneficiaries, identification of directors, promoters, proxies, UBOs, guarantors<br>**5.** Legal review of contracts<br>**6. Compliance with whistleblowing legislation** | **1. Personal details**: contact details of client or representative at client, and all information to be found on passport of a signatory or individual client (place of birth, date and place of birth, signature, ID photograph)<br>**2. Country of origin / activity**<br>**3. Copies of passport or identity cards** (and national register numbers)<br>**4. Marital status**<br>**5. Background check**: e.g. criminal activity of a board member at the client, political exposed persons' information<br>**6. Any information provided by the whistleblower to us at the time of the disclosure, or that we have collected during the verification of the reported breaches.** |
| **Performance of our contracts**<br>**1.** Provide products or services to our corporate clients or to retail clients (account opening, execution of payments, loans)<br>**2.**Exercising rights and performing our obligations under any contracts with clients<br>**3.** Performing administrative tasks related to transactions with clients, including responding to client inquiries<br>**4.** For our everyday business purposes – such as to process transactions of clients, maintain account(s), perform internal audit, or report to credit bureaus, regulators and investigators<br>**5.** Reporting trade results, asset balances, etc. to clients, including measuring or reporting business performance<br>**6.** Ensuring adequate insurance coverage<br>**7.** Facilitating NRIs in opening accounts in India | **1. Personal details**: contact details of client or representative at client, and all information to be found on passport of a signatory (place of birth, date of birth signatures)<br>**2. Copies of passport or identity cards** (and national register numbers)<br>**3. Financial details** (income, assets, investments, savings, placements, debts, loans, mortgages, credits, details of properties) |

| Purposes of the Processing | Nature of Personal Data |
|---|---|
| **Social events and marketing**<br>**1.**Client contact & maintaining relationship,<br>**2.** Offering information on services and products<br>**3.** Organising social events | **1. Personal details** (business card details)<br>**2. Information on attendance to an event**<br>**3. Pictures** (recording of images and videos) |
| **CCTV / Access**<br>**1.** Security prevention and protection<br>**2.** Ensuring evidence of security breaching actions<br>**3.** Providing physical access and managing access to our premises | **1. Personal details** (business card details)<br>**2. Pictures** (recording of images and videos) |
| **Contact with regulators and public authorities with regards to regulatory requirements, investigations, disclosure requests and / or other requests from/to regulators and public authorities as well as for lobbying and public affairs** | **1. Personal details** (business card details)<br>**2. Pictures** (recording of images and videos)<br>**3. Professional / Educational background**<br>**4. Data relating to criminal convictions and offenses**<br>**5. Copy of passport or identity card**<br>**6. Any information provided by the whistleblower to us at the time of the disclosure, or that we have collected during the verification of the reported breaches.** |

**Functioning and analysis of our Website**

1. Security and functioning of our Website
2. Analysis of visitors' browsing behaviour
3. Assisting and answering your requests in online forms (i.e. IBAN form).

1. **IP address**
2. **web browser type**
3. **operating system version**
4. **nature of the device from which you are visiting the Service**
5. **identifier for any handheld or mobile device that you may be using.**
6. **Cookies**
7. **Account number and IBAN.**