

## DATA PRIVACY NOTICE (“NOTICE”)

**Effective Date:** 6 June 2025 **Version no.:** 3.0

### THIS NOTICE

#### Company issuing this Notice

**Sumitomo Mitsui Banking Corporation, Bangkok Branch (“we”, “our”, “us” or “SMBC BKK”)** respect individual privacy and comply with all applicable privacy laws in jurisdictions in which we provide and receive services. This Notice sets out how we, as the data controller, will collect, use and disclose personal data.

In all cases, any complaints and requests to exercise data subject rights should be addressed to the Data Protection Officer Office (“**DPO Office**”) whose contact details are at the contact details set out below.

#### In this Notice:

- **“PDPA”** means Thailand’s Personal Data Protection Act B.E. 2562 (2019).
- **“Personal Data”** means any information relating to a natural person, which enables the identification of such natural person, whether directly or indirectly, but not including the information of the deceased persons in particular.
- **“Sensitive Personal Data”** means any Personal Data pertaining to race, ethnic origin, political opinions, cult, religious or philosophical beliefs, sexual behavior, criminal records, health data, disability, labor union information, genetic data, biometric data, or any data which may affect the data subject in the same manner, as prescribed under the PDPA.
- **“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, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. **“Process”** or **“Processed”** shall have a corresponding meaning.

#### To whose Personal Data does this Notice apply?

The Notice describes our practices when Processing Personal Data in the context of relationships with the following individuals (each a **“Data Subject”**, **“you”** or **“your”**):

- customers, suppliers and agents to whom SMBC BKK provides or from whom SMBC BKK receives any product or service and/or with whom SMBC BKK enters into any transaction. This includes, for example, the Personal Data of the directors, officers, board members, authorized signatories, contact persons, attorneys-in-fact, staff members or shareholders of our corporate customers;
- employees of SMBC BKK, including directors, officers, board members, staff members, shareholders and any other personnel of SMBC BKK;
- job applicants who have made a written or oral application to SMBC BKK to become employees; and
- visitors, event attendees, or any other individuals from whom SMBC BKK has collected or will collect their Personal Data throughout the course of SMBC BKK’s business activities.

## Personal Data we collect

We collect certain Personal Data in the course of providing and receiving services, and performing our business activities. We may collect the Personal Data directly from Data Subjects through communications, applications or other forms, whether we receive these in writing, verbally or electronically.

Personal Data can include:

- **Contact information** we use to communicate with the Data Subjects such as details of name (first name, last name, nickname, initial), position, current and former addresses (private and professional), telephone number (private and professional), facsimile number, email address (private and professional), emergency contact details;
- **Identity information** we use to identify, verify or authenticate Data Subjects or to meet tax, anti- money laundering (AML) and other “Know Your Client” (KYC) legal and regulatory obligations, such as details of name, address (private and professional), identification number, passport number, driver’s license number, vehicle registration number, employer, age/date of birth, nationality, gender, marital status, photograph, place of birth (City/Country), country of residence, signature, religious or philosophical belief, blood type, biometric information, height, weight, family member details, Individual Tax ID, work permit details, KYC Checklist ID, and information to assist us to determine whether the Data Subject is a Politically Exposed Person(s) (PEP or PEPs), which may include information about criminal convictions if we receive consent from the Data Subject or we are authorized to use this information under the PDPA or other relevant laws. This may extend to historical information about principals including past employment and qualifications;
- **Financial information** such as payments made and received and goods and services provided or purchased, bank account details, cheque number, credit/debit card information and financial transactions history;
- **Image capturing**, such as photographs taken at events, videos, and CCTV footage;
- **Website information** that is captured in our web logs such as device information, unique identification numbers (such as an IP address or device ID), browser information (e.g. URL, browser type, pages visited, date/time of access). This may also include information captured by any cookies and information captured on users of the website. For more details, please see our [Cookie Policy](#);
- **Communications information** including communications by email, telephone or post in the course of communicating with the Data Subjects and providing services to customers, including recordings of telephone calls;
- **Account access information** where we provide on-line account access, log-in and similar credentials, and information about use of such access;
- **Relationship information** that helps us to understand more about how to conduct business with customers, suppliers and agents, their business requirements, and what types of products and services may be of interest to customers;

- **Qualifications information** we use to assess job applicants or prospective employees' eligibility for a role or position, and that is necessary for the recruitment process such as academic background, academic certificates, language skills, training details, professional licenses, work experience and previous employments, military service status, work permit details, reference person details, credit bureau report, medical check-up report, and blacklist information; and
- **Employment information** that is necessary to manage our relationship with our employees and any other personnel, including but not limited to, job description, organizational unit, position, employment terms and conditions (e.g. salary, hours of work, overtime payment, annual leave, benefits, absence details), employee ID, account username, training records, results of assessments, criminal records, history of accusations, investigations and lawsuits, health data, social insurance information, welfare and benefits information, personal income tax information, and other information which SMBC BKK has collected or will collect throughout the course of SMBC BKK's human resources management and business administration.

For the Personal Data which SMBC BKK has collected prior to the date in which the PDPA has become fully effective, SMBC BKK will continue to collect and use such Personal Data in accordance with the Purposes (as defined below). In this regard, you have the right to withdraw your consent by contacting us at the contact details set out below. However, SMBC BKK reserves the right to consider your request for the withdrawal of consent and proceed in accordance with the PDPA.

### **Where we collect Personal Data from**

This Notice applies when we collect your Personal Data from third parties and when we collect it directly from you. We may collect Personal Data from third party sources, which include the following:

- Our corporate customers, suppliers and agents;
- Third party referrals;
- Checking and verification processes such as due diligence checks;
- Social media sites such as LinkedIn and other public internet sites;
- Credit reference agencies, insurance information bureaus and government or financial institutions.

To the extent permitted by laws, we may also collect your Personal Data from our searches of third party sources such as the press, online publications, corporate registers, sanctions lists, blacklists and databases of PEP for KYC and AML purposes.

### **How and why we use personal data**

We process the Personal Data we collect for the following purposes ("**Purposes**"):

- Facilitating smooth running of the business through communication with corporate customers, suppliers and agents, for example, to communicate about the goods and services we receive from suppliers;
- Verifying identity, checking transactions for AML purposes, assisting in the prevention of fraud, terrorist financing, bribery and corruption, tax evasion and assisting us to not provide services where Data Subjects may be subject to economic or trade sanctions, on an ongoing basis, in accordance with our AML/KYC/PEP policies;

- Credit assessment, including reviewing credit process and classification, credit renewal and credit limit set up, in order to take decisions whether to accept a customer, supplier or agent;
- Fulfilling a transaction initiated by us, such as the purchase of goods and services from suppliers;
- Fulfilling a transaction or providing a service initiated by a customer, such as application of services, bank account opening, cash deposit/withdrawal, fund transfer, cheque issuance and clearing, outward and inward remittance, and foreign exchange transactions;
- Sending communications by various methods, such as mail, email, telephone, fax and other channels;
- Maintaining and building upon relationships with customers, suppliers and agents and other business development activities;
- Maintaining business records of services, payments, acknowledgement receipts, and other transactions, including the recording and retention of voice recordings for evidentiary purposes; conducting audits for the legitimate purposes of the business; business planning and database management;
- Event management including inviting individuals to events, trainings, seminars, and visits, and conducting logistical arrangements;
- Enabling individuals to access online accounts on behalf of customers;
- Internal product analysis and market research to help us develop and improve our services to customers and to better service their accounts;
- Maintenance of our systems, resolving issues and complaints internally as soon as possible to enable us to deliver high standards of service;
- Compliance with contractual, legal and regulatory obligations and reporting requirements, including but not limited to, the PDPA, the Revenue Code, laws on financial institutions business, laws on payment system, laws on exchange control, laws on anti-money laundering, laws on labor protection, laws on offences relating to computer crimes, and other applicable laws to which we are subjected;
- Fraud and theft prevention or investigation, or other security, crime prevention or risk management purposes;
- Providing individuals acting on behalf of customers with more choices or information about products and services which may be of interest to our customers;
- Sending communications including marketing and other communications about products or services;
- Human resources management and business administration, including job application and recruitment process, scholarship program, pre-employment arrangement, work permit application, payroll management, compensation, reimbursement, tax filing, welfare, insurance, medical check-up, social benefits, survey, internal security function, training, performance assessment, investigation, punishment and resignation/retirement process;
- Internal business operation management, including ID registration for internal system, access logs record, IT system management, delegation of authority, and performance of other duties in relation to the internal business operation management;
- Maintaining and monitoring security systems, including building access control, IT systems development, usage of devices and the internet; and
- For other purposes that we informed you of at the point of collection of your Personal Data.

We justify our Processing of Personal Data under the above Purposes on any of the following lawful bases:

- Legal Obligation: performing a legal obligation to which we are subject;

- Contract: performing our obligations, or exercising our rights, under our contracts with you or in order to take steps at your request prior to entering into a contract;
- Public Task: performing a task in the public interest by us, or for the exercising of official authority vested in us;
- Legitimate Interests: pursuing our legitimate interests and those of third parties. A legitimate interest will apply only where we consider that it is not outweighed by an individual's interests or rights which require protection of their Personal Data; or
- Consent: obtaining your consent in the event when any of the above underlying lawful bases cannot be identified.

We have determined that our legitimate interests include the following:

- Managing our business and our brand;
- Maintaining business records of services, payments, acknowledgement receipts, and other transactions, including the recording and retention of voice recordings for evidentiary purposes;
- The improvement and management of relationships with customers, suppliers, agents and other Data Subjects;
- Our compliance with our regulatory requirements and improving the overall performance of the business;
- The conduct of internal audits for the legitimate purposes of managing our business;
- Administering our website, investigating any complaints, providing customer service and improving the performance and user experience of our website;
- Obtaining professional (including legal) advice to protect our business and our brand;
- The sending of communications including marketing or other communications about products or services, where this is necessary to promote our services to customers; and
- Taking steps to manage our credit, business and other risks as may be required to operate as an effective, efficient and financially prudent financial institution and where this is necessary to pursue our legitimate interests in managing and protecting our business.

If any Data Subject requires further information regarding our legitimate interests as applied to their Personal Data, please contact us at the contact details set out below.

For limited purposes, such as in the case of undertaking AML, KYC and PEP checks and related actions, it may be necessary to process Sensitive Personal Data. In these circumstances, we will process Sensitive Personal Data only when there is a lawful basis we can rely on under the PDPA. This may also include information about criminal convictions if we receive consented from you or are authorized to use this information under the PDPA or other relevant laws.

In the event that we cannot rely on the above lawful bases or the PDPA requires your consent to be provided for the Processing of your Personal Data, we will request for your consent and will only process your Personal Data once your consent is or has been provided to us.

In certain circumstances, where a Data Subject does not provide Personal Data which is required to accomplish statutory requirements or contractual obligations (for example, for us to carry out AML checks or to perform our obligations under a contract to which you are a contracting party), we will not be able to provide the products and services under our contract with such Data Subject, whether in whole or in part, or may not be able to comply with a legal obligation to which we are subject. We will make it clear if and when this situation arises and what the consequences of not providing the Personal Data will be.

## Marketing communications

If you have provided the consent to receive our marketing communications, we will keep you up-to-date with details of our services by email / post, etc. using the Personal Data that you have supplied or which we have obtained about you. You can opt out of receiving marketing as detailed below.

Additionally, we will ensure that any outside companies assisting us in marketing our products and services, or with whom we have marketing agreements, are under contractual obligations to protect the confidentiality of Personal Data, and to Process it only to provide the services we have asked them to perform, in accordance with the provisions of the PDPA.

## Who we share your Personal Data with

We will disclose your Personal Data to the following persons and entities:

- To our affiliated Sumitomo Mitsui Financial Group companies (“**SMFG group companies**”), including its management, directors, employees or relevant personnel on a need-to-know basis, for the Purposes as set out in this Notice;
- To credit reference and other third party agencies and suppliers in order to carry out anti-money laundering (AML), "Know Your Client" (KYC) and Politically Exposed Persons (PEP) checks and comply with legal obligations;
- To competent authorities such as the Bank of Thailand (BOT), the Ministry of Finance, the Revenue Department (RD), the Securities and Exchange Commission (SEC), the National Anti-Corruption Commission (NACC), courts, security or police authorities, regulators and other government agencies, where required by law or where we consider it necessary (to the extent permitted by law);
- To other commercial banks, financial institutions and business partners such as the Association of International Banks (AIB), the Thai Bankers' Association (TBA) and the Thai Bond Market Association (ThaiBMA);
- To third parties who have introduced customers, suppliers or agents to us, such as financial service providers in order to Process the Personal Data for the Purposes as set out in this Notice;
- To third parties who work on our behalf or for the customer to service or maintain customer accounts, such as administrators and managers including those external to SMBC BKK;
- To third parties who provide technical services, such as suppliers of banking applications and other IT systems, and print services, which we use to Process that Personal Data;
- To third parties in relation to human resources management and business administration of SMBC BKK such as the Ministry of Labour, the Social Security Office, insurance companies, broking services companies, hospitals, and training centers;
- To third parties who manage our physical premises;
- To third parties who service or maintain our business contact database and those who support our website;
- To third parties providing services to us such as our professional advisers (e.g. auditors and lawyers);
- To other service providers such as mailing services, delivery services, printing services, data analysis services, marketing services, or any other services which may be beneficial to the Data Subject or relevant to our business operations;
- To a party representing the Data Subjects (for example, in response to legal process); and



- Subject to applicable law, in the event that SMBC BKK and/or SMFG group companies are merged, sold, or in the event of a transfer of some or all of our assets (including in bankruptcy), or in the event of another corporate change, in connection with such transaction.

The disclosure of your Personal Data to the above persons and entities shall be in accordance with the Purposes or other purposes permitted by law. Where the law requires your consent to be provided, we will obtain your consent prior to such disclosure. SMBC BKK will put in place appropriate safeguards to protect the Personal Data that has been disclosed and to comply with the standards and duties relating to the protection of Personal Data as prescribed by the PDPA.

### **Where we will store Personal Data**

We store the Personal Data of Data Subjects set out in this Notice and documents containing such Personal Data in both physical and electronic forms in our servers, databases, vault rooms, fire proof cabinets and relevant department lockers, and, in certain circumstances, we may use external data retention service providers to store such Personal Data and relevant documents.

Furthermore, we may transfer and store the Personal Data of Data Subjects set out in this Notice on servers or databases outside Thailand, in particular to SMFG group companies. We may be required to send to SMFG group companies in Japan the names of directors, officers, board members, staff members or shareholders of its corporate customers who are Japanese nationals or non-Japanese nationals (in the latter case, whether residing in Japan or otherwise) for screening checks. In most cases, the specific countries **outside Thailand** to which SMBC BKK transfers their Personal Data are:

- Japan
- United States
- Singapore
- Malaysia
- Cambodia
- Myanmar
- United Kingdom
- Vietnam

These countries may not have the equivalent level of data protection laws as prescribed in Thailand's PDPA. If we need to transfer Personal Data outside Thailand, we will take steps to ensure that your Personal Data is protected and safeguarded at a standard of protection comparable to the protection under Thai law once it leaves Thailand to the oversea recipient. If you would like to obtain the details of such safeguards, you can request these by using the contact details set out below. In some cases, we may request your consent for the international transfer of your Personal Data, subject to the requirements under the PDPA.

### **How long we will store Personal Data for**

We will retain your Personal Data set out in this Notice for as long as required to perform the Purposes for which the data was collected, depending on the lawful basis on which that data was obtained and/or whether additional legal/regulatory obligations mandate that we retain the Personal Data. In general terms, this will mean that Personal Data will be kept for the duration of our relationship with the respective Data Subjects and:

- the period required by tax, company and financial services laws and regulations, and as prescribed under other applicable laws;
- the period during which we deem it necessary to retain Personal Data, taking into account the business practices and industry standards in relation to each category of Personal Data; and
- as long as it is necessary for Data Subjects to be able to bring a claim against us and for us to be able to defend ourselves against any legal claims. This will generally be the length of the relationship plus the length of any applicable statutory limitation period under applicable law.

In certain circumstances, Personal Data may need to be retained for a longer period of time, for example, where we are in ongoing correspondence or there is a continuing claim or investigation.

### **What are your rights in relation to the Personal Data**

Under the PDPA, a Data Subject is entitled to certain rights in relation to his/her Personal Data. Some of these rights will only apply in certain circumstances. If a Data Subject would like to exercise, or discuss, any of these rights, such Data Subject should contact the DPO Office at the contact details set out below and provide sufficient information to allow us to understand the scope of the request.

- **Withdrawal of Consent:** if our Processing is based on consent, a Data Subject can withdraw their consent at any time by contacting the DPO Office.
- **Access:** a Data Subject is entitled to ask us if we are Processing his/her Personal Data, and if we are, he/she can request access to his/her Personal Data, including to receive a copy of the Personal Data we hold about him/her and certain other information about it.
- **Correction:** a Data Subject is entitled to request that any incomplete or inaccurate Personal Data we hold about him/her be corrected.
- **Erasure:** a Data Subject is entitled to ask us to delete, destroy or anonymize his/her Personal Data in certain circumstances. There are also certain exceptions where we may refuse a request for erasure, for example, where the Personal Data is required for compliance with law or in connection with claims.
- **Restriction:** a Data Subject is entitled to ask us to suspend the Processing of their Personal Data, for example if he/she wants us to establish its accuracy or the reason for Processing it.
- **Transfer:** a Data Subject is entitled to request the transfer of his/her Personal Data to another third party in limited circumstances.
- **Objection:** where we are Processing Personal Data based on our legitimate interests (or those of a third party) a Data Subject may challenge the Processing. However, we may be entitled to continue Processing his/her Personal Data based on our compelling legitimate interests or where this is relevant to legal claims. A Data Subject also has the right to object where we are Processing Personal Data for direct marketing purposes.
- **Complaint:** If a Data Subject has any concerns or questions about the Processing of his/her Personal Data, please contact us at the contact details set out below. In case of an alleged infringement of the PDPA, a Data Subject has the right to lodge a complaint with a supervisory authority in accordance with the rules and methods prescribed under the PDPA.



The Data Subject's request for the above purposes will be proceeded within 30 days after receiving the completed information and supporting documents.

### **Changes to this Notice**

From time to time, we may change and/or update this Notice. If this Notice changes in any way, we will post an updated version on our website.

If we change anything important about this Notice (the Personal Data we collect, how we use it or the Purposes) we will highlight those changes at the top of the Notice and provide a prominent link to it for a reasonable length of time prior to the change.

We recommend you regularly review this website to ensure that you are always aware of our practices in relation to the Processing of Personal Data and any changes thereto. Any changes to this Notice will go into effect on the date such changes have been posted on this website.

### **DETAILS AND HOW TO CONTACT US**

SMBC BKK and SMFG group companies will have access to Personal Data relating to the Data Subjects set out in this Notice. However, only those data controllers who receive or provide relevant services for customers, suppliers, agents or other Data Subjects in accordance with the Purposes above will have access to their relevant Personal Data.

#### **How to Contact Us**

If you wish to exercise your rights, or to raise any questions, concerns or complaints concerning this Notice or our practices in relation to the Processing of Personal Data, you can contact us at the address below.

Our DPO Office can be contacted at:

#### **SUMITOMO MITSUI BANKING CORPORATION, BANGKOK BRANCH**

Address: 8th-10th Floor, Q. House Lumpini Building,  
1 South Sathorn Road, Bangkok 10120, Thailand  
Tel: +66 2353 8000