## Sumitomo Mitsui Trust Bank (Thai)
## Public Company Limited

# Personal Data Protection Policy

# Introduction

Sumitomo Mitsui Trust Bank (Thai) Public Company Limited ("the Bank") recognizes the importance of protecting individual rights in respect of privacy and personal data. Pursuant to this, the Bank strives to collect, use and/or disclose personal data in a manner consistent with the Personal Data Protection Act B.E. 2562 (2019) ("PDPA") that was enacted on 27 May 2019 and fully effective on 28 May 2020, the purpose of this policy is to outline the Bank's practice in relation to Personal Data processing by collecting, using, disclosing and retaining the Personal Data to ensure that the Bank will comply with the PDPA.

Unless otherwise defined, the terms used in this policy have the same meaning as ascribed to them in the PDPA.

# Definition

| Term | Prescription |
|---|---|
| Data Subject | The individual person who is the owner of the Personal Data |
| DPO | Data Protection Officer whom has been appointed by the management of the Bank and is responsible to the Personal Data Protection matter |
| Personal Data | Any information relating to a person which enables the identification of such person, whether directly or indirectly, but not including the information of the deceased persons. |
| Person | A natural person. |

# Principles

To comply with the PDPA, the Bank shall follow the principles set out below:

1. Personal Data shall be obtained lawfully in accordance with applicable laws and regulations and other obligations required by law.
2. Personal Data shall be kept for specific and legitimate purposes.
3. Personal Data shall be used and disclosed only in the specific purposes together with the clear and specific consent, if required, that obtained from the Data Subject.

4. Personal Data obtained shall be as necessary.
5. Personal Data obtained shall be accurate and up to date.
6. Personal Data shall not be held longer than necessary or requirement by any applicable laws or regulations.
7. Personal Data shall be protected subject to reasonable and appropriate security measures.
8. Personal Data shall be only communicated to third parties in line with prescribed internal policies and to extent permitted by law.

# Purpose and Use

The Bank needs to process by collecting, using, disclosing and retaining the Personal Data for the purpose of:

1. Meeting the corporate objective of the Bank.
2. Carrying out the normal operation as a Bank.
3. Maintaining good corporate governance and sound risk management.
4. Managing the human resources of the Bank.
5. Complying with laws, regulations, directives, notices and guidelines issued by government/ regulatory authorities.
6. Satisfying internal policies and procedures.

Personal Data collected may be related to the Bank's customers (including their directors, representative, staff or relevant persons), counterparties, as well as our directors, employees or potential employees (and their families) and persons and entities related to them.

Personal Data collected may be used for, but not limited to, the following purposes:

1. To perform banking-related services as a licensed bank in Thailand.
2. To carry out, monitor, manage and evaluate its business infrastructure, risk management controls and business operation as a bank in compliance with laws, regulations and guidelines issued by relevant authorities.
3. To administer, evaluate, screen and review the customers to facilitate business transactions in accordance with our risk management practices.
4. To perform audit, accounting and other record keeping functions.
5. To perform the Customer Due Diligence Anti-Money Laundering/Countering Terrorism Financing Checks.
6. To perform the recruitment, personnel, payroll and employee related functions as an employer.
7. To facilitate record keeping, storage, disaster recovery and business contingency measures.

8. To carry out the Bank's obligations in its contract with current or potential customers or business partners.
9. To respond to legal processes, pursue legal rights or remedies, defend itself in litigation and manage any complaints or claims.
10. To respond to request for information from public and government/regulatory authorities and for audit, compliance, investigative and inspection purposes.
11. To detect, prevent, investigate and report on actual or alleged fraud, misconduct or unlawful acts, including those related to money laundering or terrorism financing.

The Bank will handle Personal Data appropriately, in line with the circumstances on hand, and for lawful and targeted purposes.

# Management of Personal Data

a. Consent

The Bank shall acquire the consent of Data Subject for the process of its Personal Data in proper way otherwise it is exempted by laws or relevant regulations and the Bank must proceed it in accordance with the consent.

b. Accuracy

The Bank will do the best effort to ensure Personal Data collected is accurate and up to date.

c. Security

Personal Data within the Banks' possession or control will be subject to reasonable and appropriate physical, procedural and technological security arrangements in order to protect the risks such as unauthorized access, loss, accidental destruction, falsification etc.

d. Retention

The Bank will retain Personal Data only for as long as necessary to fulfill the purposes for which it was collected, unless a longer retention period is required for business purposes or is permitted by law.

# Disclosure

Personal Data may be shared with the Sumitomo Mitsui Trust Bank Group and/or other third parties (whether in or outside Thailand) as the Bank deems necessary and lawful for the specific purposes. Parties shared with includes:

a. Parent Bank, other branches and entities within the Group of the Bank, whether located in Thailand or overseas and their auditors, legal counsels, professional advisors and service providers.
b. Auditors, legal counsels, professional advisors and other third parties service providers (including outsourcing service providers) of the Bank.
c. Legal process participants and their advisors.
d. The Bank's insurers and medical practitioners providing medicals services to employees.
e. Public and governmental regulatory authorities, statutory boards, industry associations, law enforcement agencies, the court or alternative dispute resolution forums.
f. Any other person as required by laws or any other related regulations.

The Bank and its affiliates may use agents, contractors or data intermediaries, bound by obligations of confidentiality and data protection, in connection with performing the functions described above.

The Bank may also release Personal Data if required by law, regulation or court order.

Personal Data may be held on local, regional or global databases as permitted by the provision of PDPA and any related regulations.

# Cross Border Data Transfer

The Bank reserves the right to disclose data to entities outside of Thailand for processing in accordance with the purposes set out above. In such cases, the Bank and its employees and/or agent shall comply with the PDPA and related regulations. The Bank has implemented procedures for its employees to comply with the PDPA and related regulations. Where data in the possession of the Bank are disclosed to parties located outside Thailand, the Bank will ensure that the parties receiving the data are bound by the Bank's corporate confidentiality and data protection policies. In addition, the respective departments and staff involved in the transfer undertake that:

a. The Bank and its employees and/or agents will take appropriate steps to ensure that the Bank will comply with the obligations of the PDPA and related regulations, in respect of the transferred Personal Data while it remains in the possession or under the control of the Bank.
b. Appropriate action is taken to ascertain whether, and to ensure that, the organization receiving the data in that country or territory outside Thailand is bound by legally enforceable obligations to provide that transferred Personal Data a standard of protection that is at least comparable to that afforded by the PDPA and related regulations.
c. The Bank will ensure that the data are transferred only to countries known to have a standard of protection according to the provision of PDPA and related regulations.

# Internet/ Telephone Communication

In order to maintain the security of our systems, protect our staff, record transactions and in certain circumstances to detect crime or unauthorized activities, the Bank reserves the right to monitor any or all internet/telephone communications including all e-mail traffic into and out from its domain. Such e-mails and telephone communications constitute the property of the Bank.

# CCTV Surveillance

The Bank's premises are under surveillance by closed circuit television cameras ("CCTV") for the purpose of security measure of the bank's assets and premises and to monitor visitors' access to the Bank.

The Bank shall notify all staff, customers and visitors that their images will be monitored and captured by the CCTV as long as they are in the Bank's premises. Such notification shall be verbal, written or in the form of signs or notices placed in the Bank's premises.

# Data Subject Right

Data Subject has the right to their Personal Data as follows:

- To withdraw the consent for the collection, use or disclosure of Personal Data;
- To request an access to and obtain a copy of Personal Data or to request the disclosure of the acquisition of Personal Data obtained without consent;
- To request for obtaining Personal Data, or transferring Personal Data to the third party if it can be done by any automatic means;
- To object to the collection, use or disclosure of Personal Data;
- To request for erasing or destroying Personal Data, or anonymizing Personal Data to become the anonymous data;
- To request for restricting the use of Personal Data;
- To request for updating, completing and not misleading Personal Data collected.

Data Subject may exercise their right by contacting the DPO. All requests shall be made in writing with details to DPO together with proof of identity. Notwithstanding any withdrawal of consent, the Bank may have right to hold, use, disclose or retain the Personal Data following to any applicable laws and

regulations. If DPO refuses the request from Data Subject, DPO shall record such request of Data Subject with the reason of refusal.

For the requests for access and obtain a copy of Personal Data, DPO shall response to request within 30 days from receipt of request.

The request from the Data Subject shall be processed under the provision of PDPA and any applicable laws and regulations.

# Industry Practice

In addition to the provisions of this policy, the Bank also adheres to the established practices of the banking industry. The Bank will abide by the provisions of the rules and regulation which will be issued by regulators and any related authorities i.e. Personal Data Protection Commission or Bank of Thailand.

# Contact

Enquires about this policy, any complaints or security breaches in connection with this policy shall be made in writing or email to:

Mr. Aklavit Chongswatvorakul
Data Protection Officer
Sumitomo Mitsui Trust Bank (Thai) PCL.
98 Sathorn Square Office Tower 32nd Floor
North Sathorn Road, Silom, Bangrak,
Bangkok 10500 Thailand
Tel: +66-2230-6106
Email: Aklavit_ch@smtb.jp