

Personal Data Protection Policy

Effective Date: 01 June 2022

Siam Exchange Ltd. attaches great importance to your right to privacy and security of your personal data. Therefore, the company has prepared this policy to notify you, the Data Subject, of the purposes and details of collecting, using and/or disclosing personal data as well as your rights under the Personal Data Protection Act, B.E. 2562 (2019) (the "PDPA") and relevant laws and regulations. This will ensure that your personal data obtained by the Company will be used according to your needs and in accordance with the laws.

1. How The Company Collect, Use and Disclose Your Personal Data

The Company will collect, use or disclose your Personal Data as long as necessary only if it has a legal basis for collecting, using or disclosing personal data. This shall include the collection, use or disclosure of personal data to perform legal obligations for the legitimate interests of the Company processing with your consent and/or under other legal bases for the purposes of collecting, using or disclosing the Company's information as follows:

The Company's Legal Duties

In order to perform duties under supervision and in accordance with relevant laws and regulations, it is necessary for the Company to collect, use or disclose your personal data for any other purposes which are in compliance with laws and regulations of government agencies and/or agencies to which the Company is subject to.

- Compliance with PDPA;
- Compliance with the Anti-Money Laundering Act and the Law on the Prevention and Suppression of Terrorism Financing and Proliferation of Weapons of Mass Destruction, Verification of public information of Regulatory Authorities and/or Designated Personal Data, Know Your Customer, and Customer Due Diligence;
- Compliance with the regulations of Bank of Thailand (BOT);
- Compliance with the order of the legal authority such as court orders, etc.

Legal Contract

- Verification of Know Your Customer: Transaction information such as foreign exchange purchase and sale transactions to comply with Anti-Money Laundering Act
- Record of transaction details to comply with the regulations of Bank of Thailand (BOT)

The Company's Legitimate Interests

- Maintaining security such as images recording from CCTV inside and outside of the office area;
 - To prevent, protect or suppress a danger to life, body and belongings of a customer or those of any relevant third parties.
 - To use as evidence if there are any business transaction's problems
- Preventing, Responding and Minimizing potential risks from corruption or law violation (e.g., money laundering, terrorism and proliferation of weapon of mass destruction financing offenses related to property, life and body);
- Managing risks, Monitoring and Managing within organization.

Your Consent

The Company may request your consent to collect, use or disclose your personal data for the following purposes.

- The Company is obliged to collect, use or disclose sensitive personal data such as a photo of your national identification card which contains information of religion and/or blood type.
- Disclosure of your personal data to third parties or organizations that the Company hires as personal data processor for personal risk assessment and risk management according to Anti-Money Laundering Law.

2. Disclosure of Your Personal Data

2.1. Government agencies and Regulatory Authorities

The Company may, under applicable law, disclose your personal data as follows:

- Bank of Thailand (BOT)
 - Rules and procedures for doing business as a licensed person
- Anti-Money Laundering Office (AMLO)
 - Methods of identity verification for Financial Institutions Customers and Person Professions Section 16
 - Ministerial Regulations for Verification of Know Your Customer 2559
- Courts, Police and Legal Execution Department, etc.

2.2. The Company's External Contractors

The company may hire or contract with third parties such as personal risk processing/monitoring service providers in order to comply with the Anti-Money Laundering Law. Therefore, the Company may disclose your personal data to service providers.

However, in the event of disclosure and/or transmission of personal data to external entities, the Company must provide an appropriate personal data protection policy. The Company will not allow such external entities to use your data for any purpose other than those specified by the company.

3. Personal Data Collected, Used and/or Disclosed by the Company

Category of Personal Data	Data collected, used and/or disclosed by the company
Personal details	<ul style="list-style-type: none">- First and Last Name- Date of Birth- Government-issued documents: National ID Card, PassportWork Permits in case of foreigners / Official Identification Card / Driver's License or any other documents to identify or verify identity- Signature
Contact information	<ul style="list-style-type: none">- Current residence, address according to important documents and address of residence in Thailand and address in the country by nationality in case of foreigners- Telephone number, Email address and LINE ID
Identification details and identity verification	<ul style="list-style-type: none">- National ID Card- National ID Card Number, Passport Number- Non-Thai Identification Card- Driver's License- Signature
Work details	<ul style="list-style-type: none">- Occupation- Work address- Type of business- Position- Salary
Information contained in documents engage in transactions (Juristic Person)	<ul style="list-style-type: none">- Company Certificate- List of shareholders- Power of Attorney- Commercial Registration
Financial and transaction information	<ul style="list-style-type: none">- Channels for transactions- Transaction value, the amount of purchase, sales, foreign exchange- Income from acquisition of transaction
Audit details	<ul style="list-style-type: none">- Due diligence information (e.g., Know Your Customer KYC / Customer Due Diligence)- Audit details and risk assessment, inspection, money laundering and counter -terrorism
Security details	<ul style="list-style-type: none">- Images or moving images from closed-circuit television (CCTV)- Description of a person- Detecting suspicious or unusual activities- Images or moving images from closed-circuit television- Video recordings
Sensitive Personal Data	<ul style="list-style-type: none">- Religion- Blood type
Others	<ul style="list-style-type: none">- Record of interactions and communications between you and the Company by any means such as email, chat messages (social media), Facebook, Line, etc.- Information provided to the Company through any channels

4. Storage Duration of Personal Data

The Company shall retain Personal Data only as long as it is necessary in accordance with the requirements of the applicable law such as Anti-Money Laundering Law. As such, the Company will store your personal data for 10 years from the date of account closure or termination. The Company shall erase the Personal Data such that it cannot identify the Data Subject when the Personal Data is no longer necessary or at the end of such period.

6. Rights of Data Subject

A Data Subject is entitled to request any actions available under the provisions of the regulations and the announcements set forth now or to be amended in the future regarding his/her Personal Data as follows:

Rights	Description
Right to be Informed	A Data Subject may have the right to be informed about the processing of Personal Data collection method, parties who receive Personal Data and duration of Personal Data storage.
Right to Revoke Consent	A Data Subject may revoke his/her consent at any time.
Right of Access	A Data Subject is entitled to request access to and obtain a copy of the Personal Data related to him/her, which is under the responsibility of the Company and verify whether the process is restricted by law.
Right to Object	A Data Subject has the right to object to the collection, use, or disclosure of his/her Personal Data in addition to those required by law.
Right to Erasure / Right to be forgotten	A Data Subject shall have the right to request the Data Controller to erase or destroy the Personal Data, or anonymize the Personal Data such that it cannot identify the Data Subject.
Right to Restriction of Processing	A Data Subject shall have the right to request the Data Controller to restrict the use of Personal Data when the Company is in the process of reviewing the request to correct the Personal Data or when the Company is in the process of verifying and/or examining the Data Subject's request to object.
Right of Rectification	A Data Subject shall have the right to ensure that the Personal Data remains accurate, complete, and up-to-date.

7. Exercise channels

Siam Exchange Ltd. 422/3 Phayathai Road Wangmai Pathumwan Bangkok 10330




5. Security Measures of your Personal Data

The Company uses reasonable technical and administrative security measures to protect your Personal Data. In addition, external entities or third parties that process personal data must strictly comply with the Company's security measures and agree to maintain security of personal data.

The exercise of the rights above

may be restricted under relevant laws, and it may be necessary for the company to deny or not be able to respond to your requests, e.g., to comply with laws or court orders, public tasks, your request in breach of rights or freedom of other persons, etc. If the Company denies the request, the Company will inform you of the reason.

8. Contact Information

-  Siam Exchange Ltd.
-  02 - 2153054
-  siamexchange@hotmail.com
-  @siamexchange

