

Personal Data Protection Policy

Thanachart Capital Public Company Limited recognizes the importance of the protection of personal data (Data Privacy) of Data Subjects, which constitutes a fundamental right to an individual's privacy; and whereas a Data Subject naturally desires for their personal data to be securely and safely safeguarded; and in conjunction with the fact that personal data protection laws have prescribed rules or measures for governing and regulating the protection of personal data concerning the collection, use, disclosure of personal data, and various rights of Data Subjects. As a result, the Company has established this Policy to serve as the core principle for protecting the personal data of Data Subjects, and to provide notice regarding the details pertaining to the collection, use, and disclosure of personal data, including legal rights as a Data Subject, as follows:

1. Definitions

"Company"	shall mean Thanachart Capital Public Company Limited.
"Data Subject"	shall mean an individual who is the owner of the personal data.
"Person"	shall mean a natural person.
"Transaction" or "Executing a Transaction"	shall mean the execution of a transaction or engagement in activities with the Company, or the exercise of any legal or contractual rights that a Data Subject has with the Company, including, without limitation, participating in shareholder meetings, or receiving dividends or any other benefits from the Company.

2. Collection, Use, and/or Disclosure of Personal Data

2.1 Collection, Use, and/or Disclosure of Personal Data: The Company shall utilize lawful methods to collect, use, and/or disclose the personal data of a Data Subject. In doing so, the Company shall collect personal data on a limited basis and only to the extent necessary for the purposes of the collection, use, and/or disclosure of such personal data, and in accordance with the provisions of the law.

2.2 The Company may collect, use, and/or disclose the personal data of a Data Subject, which has been provided to or is held by the Company, or which the Company has received or accessed from other reliable sources, including, without limitation: the Department of Business Development, Ministry of Commerce; the Department of Provincial Administration, Ministry of Interior; the Department of Consular Affairs, Ministry of Foreign Affairs; credit bureau companies; the Legal Execution Department; financial institutions; and professional advisors.

2.3 In the event that a Data Subject does not provide personal data, or provides personal data that is inaccurate or not current to the Company, such circumstances may affect the Data Subject in that they may be unable to execute transactions with the Company, may experience inconvenience, or may prevent the performance of an existing contract with the Company. This may further cause the Data Subject to sustain damage or lose opportunities, and may impact compliance with any laws with which the Data Subject or the Company is required to comply.

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

The personal data collected, used, and/or disclosed by the Company is categorized into two types as follows:

3.1 General Personal Data

The Company may collect, use, and/or disclose the general personal data of the Data Subjects, categorized by the type of Data Subject as follows:

(1) Where the Data Subject is a shareholder of the Company

Given that the Company has the status of a company listed on the Stock Exchange of Thailand, and Thailand Securities Depository Company Limited (TSD), as the securities registrar, is responsible for overseeing and maintaining shareholder information as well as preparing the Company's share register book to ensure it is accurate, complete, and consistently up to date, the Company will receive the share register book from the TSD as of the book closure date. This is for the purpose of determining shareholders' statutory rights, such as the right to participate in shareholders' meetings and the right to receive dividends, among others. The share register book consists of shareholders' personal data and contact information, such as first name, last name, national identification number, passport number (in the case of foreign nationals), address, telephone number, email address, and data or channels regarding payments or other benefits. In this regard, for major shareholders as defined by law, the Company will collect additional personal data as necessary for regulatory oversight and disclosure in accordance with the criteria prescribed by law.

In addition, the Company will collect the identification information of shareholders who participate in shareholders' meetings by compiling data as it appears on copies of national identification cards, alongside the shareholder data mentioned in the preceding paragraph. This also includes proxyholders participating in the meetings, persons authorized to act on behalf of juristic persons in the case where the shareholders are juristic persons, as well as attorneys-in-fact of shareholders that are juristic persons.

(2) Where the Data Subject is a holder of the Company's debentures

In the case where the Data Subject is a holder of corporate debentures issued by the Company, the debenture underwriter or offering advisor appointed by the Company will collect the identification information of the Data Subject, as well as the contact information of the Data Subject, such as first name, last name, national identification number, passport number (in the case of a foreign national), information appearing

on copies of national identification cards, address, place of work, telephone number, fax number, and email address, among others. Such data, along with the debenture holder register, will then be forwarded to the debenture registrar appointed by the Company for further processing. The Company itself will not collect any personal data of the debenture holders.

For the personal data of holders of other types of debt securities, such as bills of exchange, the Company will collect the identification information of the Data Subject, as well as the contact information of the Data Subject, such as first name, last name, national identification number, passport number (in the case of a foreign national), information appearing on copies of national identification cards, address, place of work, telephone number, fax number, and email address, among others.

(3) Where the Data Subject is a contracting party, business partner, or contact person of the Company

The identification information of the Data Subject and the contact information of the Data Subject, such as first name, last name, national identification number, passport number (in the case of a foreign national), information appearing on copies of national identification cards, address, place of work, telephone number, fax number, and email address, among others; transaction data of the Data Subject with the Company; data or records of correspondence between the Data Subject and the Company; and data or channels regarding the payment of remuneration, funds, or any other benefits. The operations under this clause shall also include the personal data of the attorneys-in-fact of the Data Subject, or the persons authorized to act on behalf of the Data Subject in the case where the Data Subject is a juristic person.

(4) Where the Data Subject is a customer or debtor of the Company

The identification information of the Data Subject and the contact information of the Data Subject, such as first name, last name, national identification number, passport number (in the case of a foreign national), information appearing on copies of national identification cards, status, address, occupation, place of work, telephone number, fax number, and email address; transaction data of the Data Subject with the Company; data or records of correspondence between the Data Subject and the Company; and financial information of the Data Subject, such as income and expense data, debt repayment data, and asset-related data. The operations under this clause shall also include the personal data of the attorneys-in-fact of the Data Subject, or the persons authorized to act on behalf of the Data Subject in the case where the Data Subject is a juristic person.

3.2 Sensitive Personal Data, which refers to personal data that is purely personal in nature to the Data Subject under Section 26 of the Personal Data Protection Act B.E. 2562 (2019), such as religious data appearing on a copy of the national identification card (if any), legal case information provided by or involving the Data Subject, or received by the Company from existing transactions with the Company. The Company shall not maintain a policy to collect the sensitive personal data of the Data Subject, except:

(1) In the event that the Company has obtained explicit consent from the Data Subject for the purpose of identity verification of the Data Subject who applies for services and/or executes transactions with the Company;

(2) In the event of necessity for the legitimate interests of the Company (Legitimate Interest) or any other circumstances as prescribed by law.

4. Purposes of Collection, Use, and/or Disclosure of the Data Subject's Personal Data and Data Processing

The Company may collect, use, and/or disclose the Data Subject's personal data for the following purposes:

4.1 Purposes for which the Company requires consent

The Company relies on the consent of the Data Subject to collect, use, and/or disclose personal data in the following cases, unless there is a legal basis permitting the collection, use, and/or disclosure of personal data without the Data Subject's consent.

(1) The collection, use, and/or disclosure of sensitive personal data of the Data Subject for the following purposes:

(a) Religious data as shown on the copy of the national identification card (if any), for the purposes of using such copy for identity verification and authentication.

(b) Legal proceedings data provided by the Data Subject, or originating from or received by the Company through existing business transactions with the Company, for the purposes of the Company's audit and risk management.

(2) In cases where it is necessary to transfer the personal data of the Data Subject to a destination country that may not possess an adequate level of data protection, and where consent is required by the law.

4.2 Purposes for which the Company may rely on other criteria or lawful bases for collection, use, and/or disclosure of the Data Subject's personal data

The Company may rely on the following criteria or lawful bases to collect, use, and/or disclose the personal data of the Data Subject, which include:

(1) It is necessary for the performance of a contract, for entering into a contract, or for the performance of a contract with the Data Subject.

(2) It is necessary for legal compliance.

(3) It is necessary for the legitimate interests of the Company or of a third party, provided that such interests are balanced against the fundamental rights, freedoms, and interests relating to the protection of the personal data of the Data Subject.

(4) It is necessary for preventing or suppressing a danger to a person's life, body, or health; and

(5) Public interest, for the performance of a task carried out in the public interest, or for the exercising of official authority.

The Company will rely on the criteria or lawful bases in (1) to (5) above to collect, use, and/or disclose the personal data of the Data Subject for the following purposes:

- **In the event that the Data Subject is a shareholder or a debenture holder of the Company:**

The Company will take actions as necessary for the following purposes:

(a) For communication, determination of rights, or the exercise of rights of shareholders or debenture holders in accordance with the law, such as the right to participate in shareholders' or debenture holders' meetings, the right to receive dividends, returns, interest, or other forms of benefits, among others.

(b) Compliance with laws, regulations, rules, guidelines, orders, advice, and requests from regulatory authorities overseeing the Company, or competent official authorities concerned (whether domestic or international), such as the Office of the Securities and Exchange Commission (SEC), the Stock Exchange of Thailand (SET), Thailand Securities Depository Co., Ltd. (TSD), Thailand Clearing House Co., Ltd. (TCH), the Anti-Money Laundering Office (AMLO), the Department of Business Development (DBD) of the Ministry of Commerce, the Revenue Department, courts of law, among others.

(c) Minutes of meetings shall be recorded only to the extent necessary as prescribed by law or competent official authorities concerned.

- **In the event that the Data Subject is a contracting party, business partner, contact person, customer, or debtor of the Company:**

The Company shall collect, use, and/or disclose the personal data of the Data Subject as necessary for the following purposes:

(a) Contacting the Data Subject prior to the Data Subject entering into a contract with the Company.

(b) Identity verification and credit information checks, Know-Your-Customer (KYC) processes, and any verifications as necessary or as required by law.

(c) Performance of obligations under a contract between the Data Subject and the Company, or for taking actions at the request of the Data Subject prior to entering into a contract or executing a transaction with the Company.

(d) Provision of services to the Data Subject, management or review of complaints, claims, or any disputes.

(e) Valuation, registration of rights and legal acts regarding collateralized immovable property of the debtor or various assets, securing insurance for collateralized assets or life insurance for the debtor or the Data Subject.

(f) Assignment or transfer of debts or claims of the debtor or the Data Subject to other persons in accordance with the terms and conditions of any contract entered into between the Data Subject and the Company, or for the accounting or financial management of the Company.

(g) Prevention, inspection, and investigation of fraud, misconduct, or unlawful activities, regardless of whether requested by a government agency or regulatory body; and risk analysis and management.

(h) Assessment or mitigation of risks that may lead to fraudulent acts, cyber threats, or various unlawful actions.

(i) Establishment of legal claims, compliance with or exercise of legal claims, or raising a defense against legal claims, including but not limited to debt collection or the recovery of any outstanding amounts owed to the Company.

(j) Compliance with laws, rules, regulations, guidelines, orders, recommendations, and requests of regulatory bodies or competent authorities supervising the Company (whether domestic or foreign), such as the Bank of Thailand, the Securities and Exchange Commission, the Stock Exchange of Thailand, Thailand Securities Depository Company Limited, Thailand Clearing House Company Limited, the Office of Insurance Commission, the Anti-Money Laundering Office, the Department of Business Development of the Ministry of Commerce, the Revenue Department, courts, among others.

(k) Internal controls, auditing (by both internal and external auditors), business operations, and compliance with the Company's policies and procedures as may be required by applicable laws and regulations, including laws and regulations related to risk control, security, auditing, finance and accounting, various systems, and business continuity.

(l) Facilitation of financial audits to be conducted by auditors, or obtaining legal advisory services from legal advisors appointed by the Data Subject or the Company.

(m) Performance of the Company's obligations under any contracts to which the Company is a party, such as contracts with the Company's business partners, vendors, or other asset management companies, or under contracts where the Company acts as an agent.

4.3 The Company may automatically collect and record website access and usage data (Log Files) of the Data Subject, such as IP Address or type of browser (Browser), or through the use of cookies (Cookies) and similar technologies, when the Data Subject accesses the website, or uses services via the internet network or applications of the Company. This is for the purposes of analysis, website development, service provision, and tracking the use of electronic or website services, or for any other purposes, including verification in the event of usage technical issues.

In addition, the Company may use the services of third-party agencies that record access logs for website services or electronic media, for the aforementioned purposes or as required by law.

4.4 The Company will not collect, use, and/or disclose the personal data of the Data Subject for purposes other than those previously notified to the Data Subject, unless:

- (1) a new purpose has been notified to the Data Subject and consent has been received from the Data Subject; or
- (2) it is a case prescribed by law.

5. Disclosure of Personal Data

5.1 The Company shall disclose the Data Subject's personal data only in accordance with the purposes notified to the Data Subject. In this regard, the Company shall disclose the Data Subject's personal data under the following circumstances:

- (1) The Company has received consent from the Data Subject;
- (2) It is necessary for the performance of a contract or at the request of the Data Subject, including disclosure for executing transactions or any activities of the Data Subject, to enable operations to achieve the Data Subject's objectives;
- (3) It is necessary for the legitimate interests of the Company or a third party, such as disclosure to juristic persons or organizations for investigation and prevention of fraud, or for maintaining the Company's security, among others;
- (4) It is for compliance with laws, official regulations, or orders of competent regulatory authorities concerned or lawful government agencies, such as the Bank of Thailand, the Securities and Exchange Commission, the Stock Exchange of Thailand, the Thailand Securities Depository Co., Ltd., the Thailand Clearing House Co., Ltd., the Office of Insurance Commission, the Anti-Money Laundering Office, the Department of Business Development of the Ministry of Commerce, the Revenue Department, courts, or the Legal Execution Department, among others.
- (5) Disclosure to individuals, juristic persons, or any other organizations as follows:
 - (a) External service providers of the Company (Outsourced Service Providers) with whom the Company is a contractual party, such as information technology service providers, payment and/or

collection service providers, document printing or delivery/postal service providers, debt collection agencies, registrars for rights and legal acts on real estate, debtors' collateral or various assets, agents and/or brokers for the purchase or sale of assets, and securities registrars, among others;

(b) Auditors, certified public accountants, and various professional advisors, such as those providing services related to auditing, legal matters, asset valuation, accounting, and taxation;

(c) Banks providing payment systems for executing the transactions of the Data Subject, insurance companies, and/or life insurance companies in the event that the Data Subject is a debtor or a debt security holder of the Company, among others;

(d) Individuals or juristic persons that purchase debts or claims, or accept assignment of rights, or accept novation of the Data Subject, to the extent permitted under the terms and conditions of any agreements entered into between the Data Subject and the Company, or for the purpose of financial or accounting management of the Company;

(e) Government agencies or authorities with legal powers, such as the Bank of Thailand, the Anti-Money Laundering Office, the Revenue Department, the Securities and Exchange Commission, the Stock Exchange of Thailand, the Thailand Securities Depository Co., Ltd., the Thailand Clearing House Co., Ltd., the Office of Insurance Commission, the Department of Business Development of the Ministry of Commerce, courts, the Legal Execution Department, the police, or any other government agencies, among others;

(f) Assignees, transferees, or persons who may potentially be transferees in the event of a business rehabilitation, corporate restructuring, merger, acquisition, sale, purchase, joint venture, transfer, dissolution, or any similar event involving the transfer or disposition of the business, assets, or shares of the Company, whether in whole or in part.

6. Cross-Border Transfer of Personal Data

The Company does not maintain a policy of transferring the Data Subject's personal data to foreign countries. In the event that the Company is required to transfer the Data Subject's personal data to a country with inadequate personal data protection standards, the Company shall comply with the criteria prescribed by law and/or adopt necessary and appropriate measures, such as entering into a confidentiality agreement between the Company and the data recipient, among others.

7. Security of Personal Data

The Company recognizes the importance of maintaining the security of the Data Subject's personal data. In this regard, the Company has established appropriate security measures to prevent unauthorized or unlawful loss, access, destruction, use, alteration, amendment, or disclosure of personal data. This is to ensure compliance with the stipulations set forth in this Policy and/or the information technology security practices of the Company.

8. Data Subject's Rights Regarding Personal Data

8.1 In the event that a Data Subject wishes to know or request a copy of their personal data which is under the responsibility of the Company, or requests the Company to disclose the acquisition of personal data for which the Data Subject has not given consent, the Data Subject may make a request in accordance with the criteria and procedures prescribed by the Company.

8.2 In the event that a Data Subject considers any personal data related to them to be inaccurate, outdated, incomplete, or misleading, the Data Subject may request the Company to rectify such data to ensure it is accurate, up-to-date, complete, and not misleading, by making a request to the Company in accordance with its prescribed criteria and procedures.

In the event that the Company does not fulfill the Data Subject's request under the first paragraph, the Company shall prepare a record of the Data Subject's request together with the reasons as evidence for the Data Subject's inspection.

8.3 A Data Subject has the right to withdraw their consent given to the Company for the collection, use, and/or disclosure of their personal data at any time, unless there is a restriction on the withdrawal of consent by law or by a contract that benefits the Data Subject (such as when the Data Subject continues to use services or engage in transactions with the Company, or when the Data Subject still has outstanding debts or legal obligations to the Company, among others. Any withdrawal of consent shall not affect the collection, use, or disclosure of personal data for which the Data Subject has previously given consent. However, such withdrawal of consent may cause inconvenience to the Data Subject when using services or executing transactions with the Company, may restrict access to certain functionalities, or may cause the services received from the Company to be less efficient than originally intended.

8.4 A Data Subject has the right to receive personal data concerning them from the Company. In the event that the Company has arranged such personal data to be in a format which is generally readable or usable by means of automated tools or equipment, and can be used or disclosed by automated means, including:

(1) The right to request the Company to send or transfer the personal data in such format to other Data Controllers, when it can be done by automated means; or

(2) The right to directly receive the personal data that the Company sends or transfers in such format to other Data Controllers, unless it is impossible to do so due to technical circumstances.

8.5 The Data Subject has the right to object to the collection, use, or disclosure of personal data concerning them at any time in the following cases:

(1) Where the personal data is collected due to the necessity for the performance of a task carried out for the Company's public interest, or for the purpose of the Company's legitimate interests, unless:

(a) The Company can demonstrate compelling legitimate grounds that override the Data Subject's interests; or

(b) It is for the establishment, compliance, or exercise of legal claims, or the defense against legal claims.

(2) Where the collection, use, or disclosure of personal data are for the purposes of direct marketing.

(3) Where the collection, use, or disclosure of personal data are for the purposes of scientific, historical, or statistical research, unless it is necessary for the performance of a task carried out for the Company's public interest.

8.6 A Data Subject has the right to request the Company to delete, destroy, or anonymize personal data so that the Data Subject can no longer be identified, under the following circumstances:

(1) When the personal data is no longer necessary to be retained for the purposes for which it was collected, used, or disclosed.

(2) When the Data Subject withdraws consent for the collection, use, or disclosure of the personal data, and the Company has no other legal authority to continue collecting, using, or disclosing such personal data.

(3) When the Data Subject objects to the collection, use, or disclosure of the personal data pursuant to Clause 8.5 (1), and the Company cannot reject such objection request, or when the collection, use, or disclosure of the personal data is for direct marketing purposes.

(4) When the personal data has been unlawfully collected, used, or disclosed.

8.7 The Data Subject has the right to request the Company to suspend the use of personal data in the following cases:

(1) When the Company is in the process of verification at the Data Subject's request to ensure that the personal data of the Data Subject is accurate, up-to-date, complete, or not misleading.

(2) When it is personal data that must be deleted or destroyed due to being personal data that was collected, used, or disclosed unlawfully, but the Data Subject requests the suspension of its use instead.

(3) When the personal data is no longer necessary to be retained for the purposes of collection, but the Data Subject has a necessity to request its retention for the establishment of legal claims, compliance with the law, the exercise of legal claims, or the defense against legal claims.

(4) When the Company is in the process of proving overriding legitimate grounds, or for the establishment of legal claims, compliance with the law, the exercise of legal claims, or the defense against legal claims, in the event that the Data Subject exercises the right to object to the collection, use, or disclosure of the data.

8.8 The Data Subject has the right to lodge a complaint with the expert committee pursuant to the law on personal data protection in the event that the Company or the personal data processor, including employees or contractors of the Company or of the personal data processor, violates or fails to comply with the law on personal data protection or notifications issued thereunder.

In this regard, the aforementioned rights of the Data Subject are subject to various relevant factors. The Company may not be able to fulfill the Data Subject's request in cases where it is required by law, or where the personal data has been anonymized so that the Data Subject can no longer be identified, or where the Company has a legitimate interest to collect, use, and/or disclose the personal data. This includes, for example, instances where the Data Subject continues to use the services or engage in transactions with the Company, or where the Company is under a legal obligation to comply, such as retaining the Data Subject's personal data for the duration prescribed by law, or for the establishment, exercise, or defense of legal claims, even if the Data Subject has already terminated their relationship with the Company, among others.

9. Retention Period for Personal Data

The Company shall retain the Data Subject's personal data for as long as necessary to fulfill the purposes notified to the Data Subject or as specified in this Policy. In the event that the Data Subject terminates the use of services, ceases transactions, or terminates the relationship with the Company, the Company shall retain the Data Subject's personal data for a period of 10 years thereafter, or for the period required by law, applicable statutory limitation periods, or for the exercise of legal claims. Upon the expiration of such retention period, the Company shall proceed to delete, destroy, or anonymize the personal data so that the Data Subject can no longer be identified.

10. Information Regarding Third Parties

If the Data Subject provides personal data of any third parties, such as spouses, children, shareholders, directors, beneficiaries, or emergency contact details (such as the first name, last name, address, email address, and/or telephone number of such individuals), the Data Subject shall be responsible for ensuring that such individuals permit the Company to use their personal data in accordance with this Personal Data Protection Policy. In addition, the Data Subject shall be responsible for informing such individuals of this Policy and obtaining the necessary consent from the individuals concerned.

11. Updates, Reviews, or Amendments to the Personal Data Protection Policy

The Company may update, review, or amend this Policy, whether in whole or in part, from time to time, to ensure alignment with the Company's operational guidelines, laws, and regulations of competent authorities

concerned. In the event of any amendment to this Policy, the Company will promptly publish the revised version on the Company's website.

12. Links to Third-Party Websites

When using the Company's application or website, there may be links to online social networks, platforms, and other websites operated by third parties. In this regard, the Company will only provide links to websites that maintain personal data protection standards. However, the Company cannot be held responsible for the content or personal data protection standards of such other websites, unless otherwise specified. Any personal data provided by the Data Subject to such third-party websites will be collected by said third parties and will be subject to the privacy notices or policies of those third parties (if any). In such cases, the Company recommends that the Data Subject review and comply with the personal data protection policies appearing on those websites, which are separate from this Policy.

13. Contacting the Company

If the Data Subject wishes to contact the Company, has any inquiries, or wishes to request information regarding the details of the collection, use, and/or disclosure of personal data, including the rights of the Data Subject under this Policy, or wishes to withdraw consent for the collection, use, and/or disclosure of personal data, or in the event that any unauthorized use of the Data Subject's personal data is discovered, the Data Subject may contact the Company through the following channels:

Data Protection Officer :	Email address : DPO-TCAP@thanachart.co.th
Contact Address :	Thanachart Capital Public Company Limited, No. 444, MBK Tower, Floor 16-17, Phayathai Road, Wang Mai Subdistrict, Pathum Wan District, Bangkok 10330

14. Governing Law

This Policy shall be governed by and construed in accordance with the laws of Thailand. The courts of Thailand shall have exclusive jurisdiction to adjudicate and settle any disputes arising out of or in connection with this Policy.

15. Scope of Application for Personal Data Collected Prior to the Effective Date of the Personal Data Protection Act, B.E. 2562 (2019)

For personal data that the Company collected before the Personal Data Protection Act, B.E. 2562 (2019) came into full force and effect, the Company is permitted to continue collecting and using such personal data

in accordance with the original purposes. A Data Subject who no longer wishes to permit the Company to collect and use their personal data may notify the Company, indicating the withdrawal of their consent in accordance with the criteria prescribed by the Company. Any disclosure and other processing activities, apart from the aforementioned collection and use of personal data, shall strictly comply with the Personal Data Protection Act, B.E. 2562 (2019).

16. Effective Date

This Personal Data Protection Policy shall be in full force and effect from 1 June 2022 onwards.