






Specialty Natural Products Public Co., Ltd.

Personal Data Protection Policy and Practices

| Document No.: QM-SN-23 | Effective Date: 25 February 2026 | Revision No.: 02 |
|---|---|---|
|  |  |  |
| Miss Wanwisa Thongart Company Secretary | Dr. Theeraya Krisdapong Chief Executive Officer | Mr. Surapit Kirtiputra Chairman of the Board |
| Date: 25 February 2026 | Review Date: 25 February 2026 | Approval Date: 25 February 2026 |

| Rev. | Effective Date | Description of Change |
|------|------------------|--|
| 00 | 10 July 2023 | Initial creation |
| 01 | 9 August 2023 | Reviewed |
| 02 | 25 February 2026 | Annual review and update of Company Secretary name |

Personal Data Protection Policy and Practices

1. Introduction

In order to comply with the Personal Data Protection Act B.E. 2562 ("PDPA"), related subordinate legislation, and guidelines issued thereunder (collectively, "Personal Data Protection Law"), Specialty Natural Products Public Co., Ltd. ("Company") has established this Personal Data Protection Policy and Practices to serve as a guideline for protecting personal data properly, with appropriate security measures to prevent loss, unauthorized access, use, alteration, amendment, or disclosure of personal data. The Company shall review these measures as necessary or when technology changes to maintain appropriate security effectiveness.

2. Policy Objectives

2.1 To raise awareness among executives and employees of the Company regarding the importance of personal data protection and to serve as a practical guideline in compliance with Personal Data Protection Law.

2.2 To clarify the details regarding the collection, use, and disclosure ("Processing") of personal data of customers, business partners, and persons related to the Company's business, to ensure that the Company processes personal data only to the extent necessary and with appropriate care.

3. Scope of Policy

This policy covers the operations of all executives and employees of the Company, including those engaged in business relationships with the Company.

4. Definitions

"Personal Data" means information relating to a person that enables direct or indirect identification of that individual, but does not include data of deceased persons.

"Sensitive Personal Data" means personal data of a sensitive nature, including data specified under Section 26 of the PDPA, such as data relating to race, ethnicity, political opinions, religious or philosophical beliefs, sexual behavior, criminal records, health data, disability, labor union data, genetic data, biometric data, or any other data that similarly affects the data subject, as declared by the Personal Data Protection Committee.

"Data Controller" means the Company, which has the authority and responsibility to make decisions regarding the Processing of personal data.

"Data Processor" means a person or legal entity that processes personal data pursuant to instructions or on behalf of the Data Controller. Such person or entity is not a Data Controller.

"Data Protection Officer (DPO)" means a Company employee assigned to perform duties as specified under the PDPA.

5. Processing of Personal Data

5.1 Personal Data Processed by the Company

The Company may process personal data of data subjects as follows:

- (1) Identification data, such as first name, last name, title, nickname, gender, age, date of birth, nationality, national ID number, passport number, driver's license number, taxpayer ID, etc.
- (2) Contact information, such as current address, registered address, email, home telephone number, mobile phone number, etc.
- (3) Sensitive personal data, including race, religion or philosophy, customer health data, biometric data, disability, impairment, and identity. When collecting or processing sensitive personal data, the Company shall always obtain explicit consent from the data subject before or at the time of processing, unless otherwise specified by applicable law.

If the Company intends to process personal data of other types not specified in this policy, it shall notify the data subject of the details of such processing in accordance with Personal Data Protection Law.

5.2 Purposes of Personal Data Processing

Processing of personal data shall be conducted for lawful, fair, and defined purposes. The Company will process personal data only to the extent necessary for service delivery or electronic service provision within the Company's objectives. The Company shall inform and obtain consent from data subjects prior to processing, except for:

- (1) Compliance with applicable laws, such as the PDPA, Electronic Transactions Act, Telecommunications Business Act, Anti-Money Laundering Act, Civil and Criminal Codes, and Civil and Criminal Procedure Codes, etc.

Where the processing is required by law, if the data subject does not provide personal data, the Company may not be able to comply with its legal obligations.

- (2) For the benefit of an investigation by law enforcement officers or court proceedings.

(3) Where necessary for the legitimate interests of the Company or other persons or legal entities, except where such interests are overridden by the fundamental rights of the data subject.

(4) Where necessary to prevent or suppress danger to a person's life, body, or health.

(5) Where necessary for the performance of a contract to which the data subject is a party, or for the execution of pre-contractual steps at the data subject's request.

Where the processing is for contract performance or pre-contractual actions, if the data subject does not provide personal data, the Company may be unable to enter into the contract or perform obligations under the contract.

(6) To achieve purposes relating to the preparation of historical documents or archives for public benefit, or for education, research, or statistics, with appropriate safeguards in place.

6. Data Security and Quality Measures

6.1 The Company recognizes the importance of maintaining personal data security and has therefore established appropriate security measures consistent with data confidentiality requirements, to prevent loss, unauthorized access, destruction, use, alteration, modification, or unlawful disclosure of personal data, and to prevent unauthorized use of personal data.

6.2 Personal data received by the Company will be processed solely for the Company's operational purposes, and the Company will implement appropriate measures to protect the rights of data subjects.

7. Disclosure of Personal Data

The Company may disclose personal data of data subjects to external parties only for the purposes specified in this policy. Disclosure may be made to the following parties:

(1) Affiliated companies.

(2) Service providers of the Company, such as contractors, accounting firms, auditors, advisors, and/or government agencies, such as the Revenue Department, etc.

(3) Relevant external parties in the event of a change in ownership or control of the Company or its affiliated companies or any of its assets, such as in the case of a sale or merger.

8. Rights of Data Subjects

Data subjects have the right to take the following actions:

8.1 Right to Withdraw Consent

When a data subject exercises the right to withdraw consent as specified in this policy, all consents must be withdrawn in full. The Company shall inform the data subject of the consequences of withdrawal at the time of notifying the result of the withdrawal request.

8.2 Right of Access to Personal Data

The data subject has the right to request a copy of their personal data and to request that the Company disclose the source of their data. The Company may refuse such requests where required by law or court order, or where compliance may affect the rights and freedoms of other individuals.

8.3 Right to Rectification

The data subject has the right to request that the Company correct or amend their personal data to ensure it is accurate, current, complete, and does not cause misunderstanding.

8.4 Right to Data Portability

Where the Company's systems support it, the data subject has the right to receive their personal data in a format that is readable and generally usable by automated devices, or to request automatic transfer. The Company may refuse such requests where the personal data is stored for legal compliance or where the request may affect the rights and freedoms of others.

8.5 Right to Erasure

The data subject has the right to request the deletion, destruction, or anonymization of their personal data only in the following circumstances:

- (1) When the purpose for processing the personal data has ceased to exist.
- (2) When the data subject withdraws consent for processing under this policy.
- (3) When the data subject objects to processing under this policy and there are no grounds to refuse such objection.
- (4) When the personal data has been processed without a lawful basis or consent as specified in this policy.

8.6 Right to Restriction of Processing

The data subject has the right to request that the Company restrict the use of personal data in the following cases:

- (1) When the Company is in the process of verifying data following a rectification request under this policy.

(2) When the data is subject to deletion or destruction due to unlawful processing, but the data subject requests restriction of use instead.

(3) When the personal data is no longer necessary for the collection purposes, but the data subject requests retention for the establishment, exercise, or defense of legal claims.

(4) When the Company is in the process of proving that the processing of personal data has overriding legitimate grounds, or is for the establishment, exercise, or defense of legal claims, or to assess whether the processing is necessary for the Company's public interest mission, in order to rebut the data subject's objection under 8.7.

8.7 Right to Object

The data subject has the right to object to the processing of personal data relating to them in the following cases:

(1) Data that the Company collected based on necessity for public interest missions, official authority, or legitimate interests of the Company.

The Company may refuse such requests where it determines that the objection would result in non-compliance with Personal Data Protection Law, or where the matter is related to the establishment, exercise, or defense of legal claims.

(2) Cases where the Company processes personal data for marketing purposes.

(3) Cases where the Company processes personal data for research purposes as defined under Personal Data Protection Law, including statistical research. The Company may refuse if it is carrying out a mission or is required by law, or if the data has been anonymized to a degree that the data subject can no longer be identified. In such refusal cases, the Company will prepare a written explanation for the data subject.

8.8 Right to Lodge a Complaint with the PDPC Office

Data subjects may lodge complaints regarding personal data processing with the Office of the Personal Data Protection Committee ("PDPC Office") in accordance with procedures established by the PDPC Office. The exercise of rights regarding personal data shall be subject to conditions and criteria specified under Personal Data Protection Law. In certain cases, the Company may have the right to refuse to comply with the data subject's request.

9. Procedures for Collection, Use, Retention, Processing, and Destruction of Personal Data

9.1 The Company shall inform data subjects or obtain consent for processing personal data for the various purposes specified in this policy.

9.2 Processing of personal data must be in accordance with the purposes for which the data subject has given consent, except as otherwise specified in this policy.

9.3 The Company shall retain personal data only for as long as necessary for the relevant processing purposes. Retention periods shall be in accordance with the Company's confidentiality policy, IT policy, and other related policies. Upon expiry of the retention period, the Company shall delete, destroy, or anonymize the personal data.

9.4 Processing of data by various departments within the Company must be for purposes specified in this policy. Where data must be transmitted to external service providers who are data processors, the Company shall execute a Data Processing Agreement with such external service providers.

9.5 For destruction of personal data, the Company shall destroy personal data upon the data subject's request immediately, provided that such destruction does not conflict with applicable laws or other relevant necessities.

10. Incident Management in Case of Personal Data Breach

The Company has established the following guidelines for managing personal data breach incidents:

10.1 Upon detection or receipt of a complaint regarding a personal data breach, the person who detects or receives the complaint must report it to the Chairman of the Company's Data Protection Committee or the DPO for investigation, coordination with the responsible data department to identify the cause of the breach, and reporting to the relevant regulatory authorities as required by law.

10.2 Upon identification of the cause arising from:

(1) The Company's systems: Coordinate with the IT department to suspend or temporarily shut down the system for correction, or notify the external system provider to rectify the issue immediately.

(2) Internal personnel: Immediately suspend that individual's access to the data and proceed to establish an investigative committee in accordance with the Company's procedures.

(3) External service providers: The external provider shall investigate the cause and notify the Company within 5 business days from the date the Company's notification is received. In the

meantime, the Company shall temporarily suspend data transmission to that external provider until the issue is resolved.

10.3 For data that has been leaked, the Company shall manage that data to limit damage as much as possible through legal processes or other means as appropriate.

10.4 The Company shall periodically inform the complainant of the progress in damage limitation, the cause, and the preventive measures taken at each step.

11. Personal Data Protection Risk Management

The Company shall conduct a comprehensive review and assessment of personal data protection risks at least once a year by the Internal Audit department, to improve policies, processes, or procedures that are at risk of data leakage.

12. Disclosure of Compliance with Personal Data-Related Policies and Practices

The Company shall notify departments, employees, business partners, and data subjects of the policies and practices through appropriate means, such as internal and external postings or on the Company's website.

13. Compliance with Applicable Laws and Practices, and Policy Updates

The Company shall regularly monitor progress on relevant laws and guidelines, and shall periodically review and update its personal data protection policy and processes. In the event of significant changes, the Company shall notify data subjects and communicate through appropriate channels. Where applicable law requires consent from data subjects for any such changes, the Company shall obtain consent prior to the changes taking effect.

14. Related Policies

The Company has established a Confidentiality Policy that classifies all documents as confidential. Persons responsible for preparing or maintaining documents are not entitled to disclose them to external parties or to internal persons who have no role related to such documents, through any communication channel, except for internal employee coordination for the benefit of Company operations, or in cases where a relevant government authority requests disclosure in the exercise of its official functions.

15. Contact Information

In the event that data subjects wish to lodge a complaint, have inquiries or concerns regarding the processing of their personal data, or wish to exercise any rights in relation to their personal data, please contact the Company at the following details:

Specialty Natural Products Co., Ltd.

Address: 700/364 Moo 6, Nong Mai Daeng Subdistrict, Mueang Chonburi District, Chonburi Province
20000

Email: secretary@snpthai.com

Tel: 038-458698-9 Fax: 038-458697

Data Protection Officer

Address: 700/364 Moo 6, Nong Mai Daeng Subdistrict, Mueang Chonburi District, Chonburi Province
20000

Email: secretary@snpthai.com

Tel: 038-458698-9 Fax: 038-458697

16. Policy Review

Management and relevant departments shall jointly review the Personal Data Protection Policy and Practices at least once a year, to be submitted to the Board of Directors for approval.

This Personal Data Protection Policy and Practices has been approved by resolution of the Board of Directors' Meeting No. 1/2026 and shall be effective from 25 February 2026 onwards.



(Mr. Surapit Kirtiputra)

Chairman of the Board

Specialty Natural Products Public Co., Ltd.