Personal Data Protection Policy

Amendment No. 2 (Februaray 2025)

Singha Estate Public Company Limited

Prepared by	DPO Steering Group
Endorsed by	Executive Committee
Approved by	Board of Directors

Document Revision Records

Date	Revision No.	Page No.	Revision/Amendment Details	Requestor
15 May 2020	Original Issue	-	- -	-
8 Jul 2022	Amendment No. 1	1 - 5	1. Revised definitions 2. Added roles of the Board of Directors and Executives 3. Expanded the scope of policy application 4. Amended policy details 5. Violation and Breach (Removed)	DPO Steering Group
28 Feb 2025	Amendment No. 2	1-10	1. Added more clarity to the policy's objectives 2. Amended policy details	DPO Steering Group

Table of Contents

1. Introduction

Singha Estate Public Company Limited and/or its affiliates (the "**Company**") has established this Personal Data Protection Policy (the "**Policy**") to outline the principles and guidelines for its personal data processing operations. This Policy aims to create appropriate personal data protection standards that are in compliance with the Personal Data Protection Act B.E. 2562 (2019) (the "**Personal Data Protection Act**"), its subordinate legislation, and the guidelines set forth by the Office of the Personal Data Protection Committee. In addition to this Policy, the Company shall implement a personal data governance structure, work procedures, orders, announcements, guidelines, or internal operating manuals. These will contain detailed content, steps, and operational processes relating to personal data protection, supplementing the implementation of this Policy.

2. Policy Objectives

- To provide guidelines for various operations related to personal data, including the collection, use, or disclosure of personal data, as well as the rights of data subjects, the retention and destruction of personal data, and the management of personal data breaches.
- To define the scope, authority, duties, and responsibilities of the Company's personnel, the Data Protection Officer, and the DPO Steering Group in accordance with the Personal Data Protection Act.

3. Definitions

Any term or phrase used in this policy shall have the following meanings, unless otherwise specified or explained herein.

Term/Phrase	Definition
Person	Natural person.

Term/Phrase	Definition
Personal Data	Information relating to a person which enables the identification of such person, whether directly or indirectly, but not including the information of the deceased specifically (referenced from the Personal Data Protection Act).
Sensitive Data	Personal data that is sensitive and if disclosed, could lead to unfair discrimination or affect the rights and freedoms of the data subject, requiring special care in its processing. This includes data concerning race, ethnicity, political opinions, religious or philosophical beliefs, sexual behavior, criminal records, health data, disability, labor union data, genetic data, biometric data, and any other data as prescribed by the Committee.
Personal Data Processing	Any operation or set of operations performed on personal data, whether or not by automated means, such as collection, use, disclosure, transfer, organization, structuring, storage, deletion, alteration, consultation, disclosure by transmission, dissemination, making available, alignment, combination, restriction, erasure, or destruction.
Data Controller	A natural or legal person who has the authority to make decisions regarding the processing of personal data.
Data Processor	A natural or legal person who processes personal data on behalf of or under the instruction of the Data Controller. It is understood that such a natural or legal person is not considered a Data Controller.

Term/Phrase	Definition
Data Subject	The government agency responsible for and overseeing personal data protection.
Third Party	A natural or legal person to whom the Company discloses, receives, or transfers personal data, such as outsource service providers, consulting firms, contractors, sales agents, marketing companies, business partners, and recruitment agencies.
Office of the Personal Data Protection Committee	The government agency responsible for and overseeing personal data protection.
Data Protection Officer / DPO Working Team : DPO	The Company's Data Protection Officer or Data Protection Working Team
DPO Steering Group	The internal Data Protection Steering Group that provides guidance for decision-making regarding the Company's personal data protection
Employee	An employee of Singha Estate Public Company Limited and/or its subsidiaries, including permanent, contract, temporary, and daily employees

4. Roles

The Company establishes the following governance structure to ensure operations are in accordance with this Policy:

Function/Personnel	Duties and Responsibilities
Board of Directors	Oversee the establishment of a personal data governance structure and related internal controls, and monitor and support the Company's efficient and legal implementation of personal data protection.
Executives	Monitor and ensure that the responsible departments comply with the Company's Personal Data Protection Policy and promote awareness among employees.
DPO Steering Group	Endorse policies and operational procedures, and approve operational manuals relating to the Company's personal data protection. Provide guidance for decision-making regarding personal data protection to the Data Protection Officer and the Data Protection Working Team to ensure consistency across all business units.
Data Protection Officer / DPO Working Team (DPO)	Develop and review policies, operational procedures, operational manuals, and other documents relating to personal data protection. Provide consultation to the Data Controller, the Data Processor, and all employees, including taking action to protect the rights of data subjects such as reviewing requests to exercise rights or complaints regarding personal data breach incidents.
Employees	Comply with the Company's Personal Data Protection Policy and other documents relating to personal data protection.

5. Scope of Policy Enforcement

This policy applies to the Company's Board of Directors, executives, and employees of all

departments, who operate within the scope and objectives of the Company, including the processing of personal data by external parties who process personal data under the instruction or on behalf of the Company, unless otherwise specified in this policy.

6. Principles of Personal Data Protection

Personal data processing must adhere to the following principles:

6.1 Lawfulness, Fairness, and Transparency

Personal data processing must be conducted lawfully, fairly, and transparently.

6.2 Purpose Limitation

Personal data processing must be limited to specified and legitimate purposes and must not be used or disclosed beyond those purposes.

6.3 Data Minimization

Personal data must be collected only to the extent that it is adequate, relevant, and necessary for the specified purposes.

6.4 Accuracy

Personal data processed must be accurate and kept up to date.

6.5 Storage Limitation

Personal data must be kept for no longer than is necessary for the purposes for which it is processed.

6.6 Integrity and Confidentiality

Personal data processing must be conducted with regard to the security of personal data through the use of appropriate technology and measures.

6.7 Accountability

The Company, as the Data Controller, is responsible for complying with the measures related

to the principles of personal data protection as outlined in this policy.

7. Bases for Processing Personal Data

7.1 In processing personal data, the Company must be able to rely on at least one of the legal bases specified in the Personal Data Protection Act as follows:

7.1.1 Consent Basis

7.1.2 Basis for the preparation of historical documents or archives for public interest, research, or statistics

7.1.3 Basis for preventing or suppressing danger to the life, body, or health of a person

7.1.4 Basis for the performance of a contract to which the data subject is a party, or to take steps at the request of the data subject prior to enteringinto a contract

7.1.5 Basis for carrying out a mission for public interest or exercising state authority granted to the Company

7.1.6 Basis of legitimate interests of the Company or other persons, provided that such interests do not override the fundamental rights and freedoms or the interests of the data subject, and do not impose undue burdens or unfairness on the data subject

7.1.7 Basis for compliance with the Company's legal obligations

7.2 In processing sensitive personal data, the Company must be able to rely on at least one of the legal bases specified in the Personal Data Protection Act as follows:

7.2.1 Explicit Consent Basis

7.2.2 Basis for preventing or suppressing danger to the life, body, or health of a person, where the data subject is incapable of giving consent

7.2.3 Basis for carrying out lawful activities by foundations, associations, non-profit organizations, or labor unions

7.2.4 Basis for data made public with the explicit consent of the data subject

7.2.5 Basis for the establishment of legal claims

7.2.6 Basis for compliance with laws for the achievement of objectives related to preventive medicine, occupational medicine, public health, labor protection, social security, national health security, medical welfare, scientific, historical, or statistical research, or other important public interests.

8. Privacy Notice

The Company has established the following guidelines for privacy notices:

8.1 The Company shall establish processes and methods for issuing Privacy Notices to inform data subjects of the details regarding the Company's personal data processing, prior to or at the time of collecting personal data.

8.2 Privacy Notices must include at least the following information as required by the Personal Data Protection Act:

8.2.1 The purposes and legal bases for processing personal data

8.2.2 The personal data collected and the retention period for such personal data

8.2.3 The sources of personal data, such as collection directly from the data subject or from other reliable sources

8.2.4 The persons or entities to whom personal data may be disclosed

8.2.5 The contact information and methods for contacting the Company, its representative, or the Company's Data Protection Officer (if any)

8.2.6 The rights of data subjects under the Personal Data Protection Act

8.3 The Company shall establish appropriate channels for issuing Privacy Notices, whether through electronic channels or via contact with employees, representatives, or any other

persons acting on behalf of the Company. This is to ensure that data subjects are informed of the Company's privacy notice.

8.4 The Company shall update or amend the Privacy Notice to reflect current personal data processing practices and shall regularly review the details of the privacy notice. All updates or amendments to the Privacy Notice shall be recorded as evidence for auditing purposes.

9. Consent Acquisition

9.1 When requesting consent, the Company must comply with the following requirements:

9.1.1 The consent request must clearly state the purposes of processing personal data, and must not be deceptive or mislead the data subject regarding those purposes.

9.1.2 The consent statement must be clearly separated from other texts and must not be included as part of a contract or terms and conditions of service.

9.1.3 The language used must be clear and easy to understand.

9.1.4 The data subject must be given the freedom to grant consent.

9.1.5 Consent may be obtained in writing or through electronic systems, unless the nature of the situation precludes such methods.

9.2 The data subject may refuse to give consent or withdraw consent at any time, according to their wishes.

10. Measures to Support Data Subject Rights

10.1 The Company shall provide channels for receiving requests related to the exercise of data subject rights under the Personal Data Protection Act, to facilitate data subjects.

10.2 The Company shall establish timeframes for complying with data subject requests and for notifying data subjects of the results of such requests without undue delay.

10.3 In the event that the Company rejects a data subject's request, the Company shall maintain

a record of the rejection, including the reasons for the rejection and the personal data processing activities that were denied, as evidence for auditing purposes when requested by the Office of the Personal Data Protection Committee or the data subject.

11. Personal Data Breach

11.1 The Company shall provide channels for reporting personal data breaches, processing to respond to requests, and establish guidelines for actions to be taken in the event of a breach affecting data subjects. All of this must be in accordance with the standards prescribed by the Personal Data Protection Act and its related subordinate legislation.

11.2 In the event of a personal data breach, the Company shall immediately assess the impact on data subjects upon becoming aware of the incident. If the breach poses a risk to the rights and freedoms of individuals, the Company shall promptly notify the Office of the Personal Data Protection Committee and the affected data subjects (as applicable), along with the remedial measures. This shall be done in accordance with the standards prescribed by the Personal Data Protection Act and its related subordinate legislation.

12. Security Measures

The Company shall implement appropriate organizational and technical security measures for personal data, adhering to the principles of confidentiality, integrity, and availability, to prevent unauthorized loss, access, use, alteration, modification, or disclosure of personal data. These measures shall comply with the standards set forth in the Personal Data Protection Act and its related subordinate legislation.

13. Employee Training Guidelines

13.1 The Company recognizes the importance of employee training to ensure employees understand and comply with personal data protection practices. This aims to prevent personal data breaches or any non-compliance with the Personal Data Protection Act. Current employees must undergo regular training on personal data protection, at least annually. The

Company shall provide accessible channels for employees to inquire about compliance with the Personal Data Protection Act, this policy, and any other related Company regulations concerning personal data protection.

13.2 All executives and employees of the Company are required to ensure that their responsibilities align with the Company's Personal Data Protection Policy, including all related regulations and documents.

14. Policy Review

The Company shall review and revise this policy at least annually or when significant changes occur.

Announced on 28 February 2025

(Mr. Petipong Pungbun Na Ayudhya)

Chairman of the Board of Directors