Personal Data Protection Policy

Stecon Group Public Company Limited

Content

1. Introduction

Stecon Group Public Company Limited and its affiliates recognizes the importance of protecting the personal data of the Company's directors, executives, employees, customers, business partners and business-related persons under the Personal Data Protection Act B.E. 2562 (2019) (including its amendments) and other relevant laws to prevent damage caused by the misuse or fraudulent exploitation of personal data.

This is to ensure that the Personal Data Protection Policy is in line with the law or international standards that have changed. The Company may make changing to this Policy without prior notice or notice. Nevertheless, the Company will disseminate changing to the Personal Data Protection Policy through various channels and notify the Company's supervisory authority for acknowledgment

2. Definition

Personal Data	means	Personal data as defined by the Personal Data Protection Law such as name, surname, nickname, address, telephone number, ID number, driver's license number, bank account number, credit card number, car registration, land deed, email address, IP address, cookie ID, log file, etc.
Sensitive personal data	refers to	Information that is inherently personal to an individual but is sensitive and may be subject to unfair discrimination such as race, ethnicity, political opinion, creed, religion or philosophy, sexual behavior, criminal record, health and disability information, trade union information, genetic information, biological information or any other information that affects the Data Subject in the same way as specified by the Company's office
Person	means	An individual
Data Subject	means	A person who can be identified from personal data
Company	means	Stecon Group Public Company Limited and its affiliates
Office	means	The Office of the Personal Data Protection Commission

3. Processing of Personal Data

The Company is obliged to comply with the principles for processing personal data as following

3.1. Processing personal data is only as necessary for the Company's clear and lawful purposes. It must be able to refer to at least one of the lawful bases under the Personal Data Protection Law. The Company must also be able to refer to at least one of the special conditions of the processing under the Personal Data Protection Act.

3.2. Inform the Data Subject of the purpose of processing the Personal Data in accordance with the Personal Data Protection Law and only process personal data within the scope of the purpose as notified to the data subject. Anyway, The Company may process Personal Data other than the original purpose as notified to the Data Subject only if it can refer to the Lawful Basis as required by the Personal Data Protection Law or in case it is necessary to obtain the consent of the Data Subject. The Company must also notify the new purpose and obtain the consent of the Data Subject before processing the Personal Data.

3.3. If consent is necessary, the Company will determine the channel for the Data Subject to provide consent appropriately and withdraw consent easily whether the act is done through electronic channel or through any other channels including the need to notify each other of the impact. It may also be caused by notifying the data subject of the cancellation of consent.

3.4. In case that the Personal Data of the Data Subject is restricted in its powers such as minor, incompetent person or virtually incompetent person, the Company must act in accordance with the Civil and Commercial Code and the Personal Data Protection Law.

3.5. Establish the operational procedure for the protection of personal data sent or transferred to foreign country or foreign organization. The recipient country must have adequate personal data protection standard and comply with the criteria for providing protection for personal data sent or transferred abroad or as required by personal data protection laws. In case of sending or transferring personal data, it is a transfer within the same business group or business chain located abroad. The Company may transmit or transfer information in accordance with the Company's Personal Data Protection Policy which must be reviewed and certified by the Company's office.

3.6. Retain personal data only as necessary for the purpose of processing such personal data until the data subject terminates the relationship with the Company. The Company will continue to retain Personal Data for the period prescribed by law or for the period specified by the Company's internal policy or regulation for a specific purpose. The Company will arrange for the verification of the deletion or destruction of personal data and the deletion or destruction of personal data in accordance with the rule on deletion or destruction of personal data at the end of the necessary period for the purpose of processing personal data or the end of the retention period of personal data or any other case prescribed by the Personal Data Protection Law.

4. Data Protection Officer

In case that the Company is obliged under the Personal Data Protection Law to appoint a Data Protection Officer (DPO), the Company must appoint a Data Protection Officer who must have knowledge and understanding of the Personal Data Protection Law and be independent in performing its duty and the

Company must provide adequate tool or equipment, as well as facilitate access to Personal Data for the performance of duty for the Personal Data Protection Officer.

The Data Protection Officer will be responsible for determining and monitoring the implementation of this Policy and the Internal Operating Procedures in order to ensure that the Company's processing of Personal Data complies with the Personal Data Protection Laws as well as providing advice and opinion to various departments and employees of the Company regarding the compliance with this Policy and the Internal Operating Procedure. In addition, the Data Protection Officer must coordinate and cooperate with the Office in case of a problem is related to the Company's processing of personal data and report directly to the Chief Executive Committee as well if that problem is in the performance of its duty under this Policy. The Company will also maintain the confidentiality of the personal data that it has known or obtained in the performance of its duty under this Policy.

5. **Rights of Data Subject**

Data subject has the right to take action related to their personal data. This is in accordance with the Personal Data Protection Act B.E. 2562 (2019) and other relevant laws, including the right to access and obtain a copy of personal data related to them. The right to request personal data related to oneself correction Objection to the processing of personal data Suspension of use, request for deletion/destruction of one's own personal data, including request for disclosure of the acquisition of personal data without the consent of the data subject.

6. **Contact Channel**

If the Data Subject wishes to contact the Company or wishes to exercise the right of the Personal Data, he or she may contact the Company at:

Address : Stecon Group Public Company Limited

32/59-60 Sino-Thai Tower, 29th-30th Floor, Sukhumvit 21 Road (Soi Asoke)

Khlong Toei Nua, Wattana, Bangkok 10110

Tel : 02-610-4900 Ext. 1668

Email : pdpa@stecongroup.co.th

7. **Personal Data Security Measure**

The Company has measure to protect personal data to prevent unauthorized use or disclosure of personal data as following

7.1 Audit and assess risk related to the security of the process and system of retaining personal data both information technology systems and document at least once a year in order to review and

develop and improve security measure related to the retention of personal data in accordance with the minimum standard set by the Office.

7.2 Clearly define the rights of persons who have the right to access personal data. The level of access to information is divided according to duty and responsibility, work and necessity.

7.3 Stipulate clear penalty for offense related to the processing of personal data that are not in accordance with the Personal Data Protection Act B.E. 2562 (2019) and other relevant laws.

7.4 Raise awareness among relevant personnel. The importance of using, disclosing and preserving personal data, relevant law, good corporate governance policy, business ethic and penalty through training, seminar, meeting and communication through various channels of the Company, etc.

8. Measure to support the exercise of rights of data subject

The Company will provide a channel to receive requesting for the exercise of the rights of the Data Subject in order to facilitate the data subject. A central agency must be arranged to be responsible for considering the data subject's requesting to exercise his or her rights before processing that requesting. The Company will also determine the period for complying with the Data Subject's requesting for exercise of rights and notify the data subject of the result of the compliance with the requesting without delay. In addition, it must be arranged to record the management of personal information. In case there is a rejection of the requesting to exercise the rights of the data subject to be used as evidence when the Office or the Data Subject also requests it.

9. Notification of Personal Data Breach

9.1. In case that any employee or department finds that the information technology system or related procedures are not functional, the employee or the agency that encounters such incident will immediately or within any other period as specified in the Internal Operating Regulations and the relevant agency will coordinate with the Personal Data Protection Officer (if any) or the supervisory authority to take appropriate action.

9.2. The Data Protection Officer (if any) or supervisory authority will then investigate all incidents related to the Personal Data Breach in order to take appropriate measure to mitigate the impact and prevent future Personal Data Breach. The Company will notify the Personal Data Breach to the Data Subject and the Office as required by law in accordance with the following rules.

Impact on the rights and freedoms of data subject	Operation
In case there is no risk	- Log personal data breach incident
In case of risk	- Log personal data breach incidents

	- Notify the office within 72 hours.
High risk case	- Log personal data breach incidents - Notify the office within 72 hours. - Notify the Data Subject along with remedial instructions as soon as possible.

10. Penalty

The punishment of the offender will be in accordance with the Company's regulations and in accordance with the law.

This Personal Data Protection Policy was approved by the Board of Directors Meeting No. 2/2024 on February 27th, 2024 and be effective from February 27th, 2024 onwards.

Promulgated on 27th February 2024

_____

(Mr. Vallop Rungkijvorasathien)

Chairman of the Board of Directors

Stecon Group Public Company Limited