- Translation -

Personal Data Protection Policy

Bangchak Sriracha Public Company Limited ("Company") recognizes the criticality of personal data protection and alignment with the Personal Data Protection Act (PDPA) of 2019 and applicable laws, the Company hereby defines a Data Protection Policy to guide its supervision and management of personal data collected, used, or disclosed under the law. Below are the essences of this policy.

1. All directors, executives, employees, and temporary hires of the Company and third-party agencies serving the Company must strictly abide by data protection laws, policies, regulations, requirements, manuals, and guidelines issued by the Company.

2. All directors and executives must promote awareness by employees, temporary hires, and third-party agencies serving the Company of the criticality of personal data. They must also promote proper risk management as well as security measures concerning personal data at all levels of the organization.

3. The Company has appointed Data Protection Officers (DPOs) to guide, consult, and audit operation concerning collection, application, or disclosure of data by the Company in line with the PDPA of 2019 and applicable laws. DPOs also coordinate with and extend cooperation to the Office of the Personal Data Protection Committee.

4. Directors and executives must support DPOs in performing the tasks by providing adequate tools or equipment as well as facilitate the access to the Personal Data to perform the duties.

5. The collection of personal data shall be limited to the extent necessary in relation to the lawful purpose of the data controller.

6. Collection, use, or disclosure of personal data must have explicit consent from data subjects prior to or at the time of such collection, use, or disclosure, except the case where it is permitted to do so by the provisions of the Personal Data Protection Act (PDPA) B.E. 2562 (2019) or any other laws. These details consist of data collection objectives, necessity or impacts resulting from non-permission, details of personal data to be stored, period of storage/retention, types of parties or agencies that could receive personal data, the Company's data (the Personal Data Controller), data for DPO contact, and legal rights of personal data subjects. Exceptions apply to data collection, application, or disclosure that needs no consent as specified by the law.

7. Collection, use, or disclosure of personal data must be done under the objectives stated to data subjects prior to or at the time personal data are being collected except where specified otherwise by the law. No personal data are to be collected from non-owners. Exceptions apply where notification has been promptly made to data subjects who grant the consent or where legitimately exempted.

8. The Company must take into consideration the rights of data subjects (Privacy by design) from work processes to work system development through product and service design. The Company must always maintain an establishment of security of personal data security measures by leveraging proper as well as adequate technical and management measures.

9. The Company must ensure that the personal data remains accurate, up-to-date, complete, and not misleading. It must require all units to collect and record processing activities (Data Inventory) under legitimate criteria and methods so that data subjects and the Personal Data Protection Office may audit them.

10. The Company must maintain the confidentiality and provide appropriate security measures for preventing the unauthorized or unlawful loss, access to, use, alteration, correction or disclosure of personal data, and such measures must be reviewed when it is necessary, to efficiently maintain the appropriate security and effectiveness of data security as required by law.

11. The Company must put in place the examination system for deletion or destruction of the Personal Data when the retention period ends, or when the Personal Data is irrelevant or beyond the purpose necessary for which it has been collected except storage for legitimate objectives.

12. If the Company commissions third-party individuals or agencies to process personal data for itself, it must institute an agreement to control the performance of data processors in line with the PDPA of 2019. It must also prevent such third parties from unlawful collection, use, or disclosure of personal data disclosed or transferred by the Company.

13. The Company must accommodate the lawful rights of data subjects should they demand exercise of such rights. It must also institute an audit system for such action. Prompt efforts must be made at the requirement of data subjects within periods specified by law.

14. The Company must notify the Office the Personal Data Protection Committee of any personal data breach without delay and, where feasible, within 72 hours after having become aware of it, unless such personal data breach is unlikely to result in a risk to the rights and freedoms of the persons. If the personal data breach is likely to result in a high risk to the rights and freedoms of the persons, the data controller shall also notify the personal data breach and the remedial measures to the data subject without delay.

15. If the Company needs to send or transfer personal data to foreign countries, the destination countries or international organizations that receive such personal data shall have adequate data protection standard.

16. The Company must ensure that government agencies or organizations assigned to apply government power ("government agencies") gain access to personal data only were stated by law. Without such power, the Company must not allow access or disclosure of personal data since it will be held liable for such unlawful disclosure. In addition, the Company must arrange for identification of government officers

before granting access or allowing disclosure of personal data to government agencies. Finally, it must prepare complete records of related items.

17. The Company has required that all units cooperate with the Office of the Personal Data Protection Committee when requested to forward documents or data concerning whistleblowing matters or other matters concerning personal data protection. Also, it has required that such units clarify facts about such matters at the advice of DPOs.

This policy is to be understood and observed by all directors, executives, employees, temporary hires, and third-party agencies serving the Company, with guidelines under the Personal Data Protection Policy in the attachment. All executives must provide role models by supporting and driving the policy to strict implementation.

Mr. Bundit Hansapaiboon

Chief Executive Officer