708/2568

25 November 2025

Saksiam Leasing Public Company Limited
Personal Data Protection Policy

Saksiam Leasing Public Company Limited and its subsidiaries (the "Company") recognize the importance of and are committed to maintaining the security of personal data. In accordance with the Personal Data Protection Act B.E. 2562 (2019), including any amendments thereto (the "PDPA"), the Company has therefore established the following Personal Data Protection Policy:

1. Definitions

Personal Data: any information relating to a person, which enables the identification of such person, whether directly or indirectly, but not including the information of the deceased persons in particular, in accordance with the Personal Data Protection Act.

Data Subject: the individual who is the subject of the personal data. The data subject refers only to a natural person and does not include a "juristic person" established by law.

Data Controller: a person or a juristic person having the power and duties to make decisions regarding the collection, use, or disclosure of personal data.

Data Processor: a person or a juristic person who operates in relation to the collection, use, or disclosure of personal data pursuant to the orders given by or on behalf of a Data Controller. However, such person or juristic person who performs such actions is not the Data Controller.

2. Objectives for Collecting, Storing, and Using Personal Data

The Company will collect, store, and use personal data for the benefits of providing services, market research, organizing promotional activities, or for the benefit of creating a database and using the data to offer privileges according to interests, or for the benefit of analyzing and offering any services or products of the Company and/or persons acting as representatives or related to the Company and/or other persons, and for any other purposes not prohibited by law, and/or to comply with laws or regulations applicable to the Company. This includes the transmission, transfer, and/or disclosure of personal data to subsidiaries, external service providers, data processors, assignees, or any entities having contracts with the Company.

The Company will retain such data only for the period necessary to fulfill these purposes. Such actions shall be in compliance with the Personal Data Protection Act. If there is a subsequent change in the objectives for collecting personal data, the Company will notify the Data Subject accordingly.

3. Sources of Personal Data

In carrying out its mission and operational objectives, the Company will collect data directly from the Data Subject. Authorization to act on behalf of the Data Subject is permissible; however, the authorized person must present accurate and complete evidence of authorization. The Company does not collect the Data Subject's personal data from other sources.

4. Consent and/or Disclosure of Personal Data

In collecting, using, or disclosing personal data, the Company will request prior consent from the Data Subject on every occasion, except in exempted cases as prescribed by the Personal Data Protection Act (PDPA) or other applicable related laws. The request for consent shall be made explicitly, in writing or via an electronic system (unless it cannot be done by such methods by its nature). In this regard, the Company will inform the Data Subject of the purposes for collecting, using, or disclosing the personal data along with the request for consent. Furthermore, the Company will not impose conditions for giving consent to collect, use, or disclose personal data that are unnecessary or unrelated to entering into a contract or receiving any services from the Company.

5. Exceptions to Requesting Consent from the Data Subject

The Company shall establish and maintain the lawful and fair collection of personal data, collecting only as necessary to provide services according to the Company's objectives and as prescribed by law. The Company will not collect personal data without the consent of the Data Subject, except in the following cases:

5.1 To comply with laws applicable to the Company, such as the Personal Data Protection Act, the Electronic Transactions Act, and the Anti-Money Laundering Act.

5.2 To prevent or suppress a danger to a person's life, body, or health.

5.3 It is necessary for the performance of a contract to which the Data Subject is a party, or in order to take steps at the request of the Data Subject prior to entering into a contract.

5.4 It is necessary for the performance of a task carried out in the public interest by the Data Controller, or it is necessary for the exercising of official authority vested in the Data Controller.

5.5 It is necessary for the legitimate interests of the Data Controller or any other persons or juristic persons other than the Data Controller, except where such interests are overridden by the fundamental rights of the Data Subject regarding their personal data.

5.6 To achieve purposes relating to the preparation of historical documents or archives for public interest, or for purposes relating to research or statistics, provided that appropriate safeguards are implemented to protect the rights and freedoms of the

Data Subject, as will be further prescribed in relevant notifications issued under the Personal Data Protection Act.

6. Security Measures

The Company realizes the importance of maintaining the security of personal data. The Company has established appropriate security measures for personal data that align with the confidentiality of personal data to prevent loss, unauthorized or unlawful access, destruction, use, alteration, modification, or disclosure of personal data, as well as to prevent the unauthorized use of personal data. This is in accordance with the Company's announcement regarding the Cybersecurity Policy and complies with the ISO/IEC 27001 information security standard.

In this regard, the personal data the Company has received—such as name, age, address, telephone number, identification card number, financial information, family members, etc.—which can identify the data subject, and which is accurate and up-to-date personal data, will only be used in accordance with the Company's operational objectives and under relevant laws. Furthermore, the Company will implement appropriate measures to protect the rights of the data subject.

Data Breach Notification

The Company will establish measures to detect and report personal data breach incidents. If an incident is found that may affect the rights of the data subject, the Company will notify the Office of the Personal Data Protection Commission within 72 hours and notify the data subject without delay, along with specifying remedial guidelines.

7. Restrictions on Data Usage and Data Quality

The Company will not use or disclose personal data without the prior consent of the data subject, except for personal data that can be collected in accordance with Clause 4 of this policy or any other provisions specified by the Personal Data Protection Act (PDPA). The Company places importance on the accuracy, completeness, and up-to-date nature of the data.

The Company may use the information technology services of a third-party service provider to maintain personal data. Such service providers must have security measures in place and are prohibited from collecting, using, or disclosing personal data beyond what the Company specifies. In all cases, such operations must strictly comply with the Personal Data Protection Act (PDPA).

8. Retention Period and Destruction of Personal Data

The Company will retain the personal data of the data subject for the retention period that has been explicitly notified to the data subject. The Company will periodically review the data destruction schedule, and once the specified retention period has elapsed, the Company will immediately proceed to destroy the personal data or anonymize it so that the data subject can no longer be identified.

9. Rights Regarding Personal Data

The data subject has the right to withdraw consent, the right to access data, the right to erase data, the right to restrict the use of data, the right to data portability, the right to object to data processing, and the right to request a copy of their personal data under the Company's responsibility, or request the Company to disclose the acquisition of such personal data in accordance with the criteria and methods specified by the Company. This includes the right to request corrections or modifications to ensure the data is accurate and up-to-date. However, the Company may reject the data subject's request as stipulated by law or a court order if the exercise of such rights may cause damage to the rights and freedoms of others.

10. Data Protection Officer and Employees

The Company will appoint a Data Protection Officer (DPO) to monitor the Company's operations regarding the collection, use, and disclosure of personal data to ensure compliance with personal data protection laws, including other relevant laws related to personal data protection. In this regard, the Company will support the performance of the Data Protection Officer by providing adequate tools or equipment, as well as facilitating access to personal data for the execution of their duties. The Company communicates and encourages employees at all levels to receive regular training on personal data protection to build awareness and a corporate culture that respects the personal data rights of customers, business partners, and employees, ensuring they understand the impact on the organization if the Personal Data Protection Act is not strictly followed.

11. Responsibilities of Persons Involved in the Collection, Storage, Use, and Disclosure of Personal Data

The Company requires that individuals involved in the collection, storage, use, and disclosure of the data subject's personal data prioritize and take responsibility for the storage and protection of the personal data they handle, and they must strictly adhere to the Company's established Personal Data Protection Policy.

12. Communication Channels with the Data Controller

The data subject can communicate with the Company via the following channels:

12.1 Data Protection Officer (DPO): Mr. Pithak Takham

12.2 Head Office: Saksiam Leasing Public Company Limited, No. 49/47, Jetsadabodin Road, Tha It Subdistrict, Mueang Uttaradit District, Uttaradit Province 53000

12.3 Telephone: 088-7764049, 065-4727093

12.4 Email: dpo@saksiam.co.th

13. Enforcement

In the event that the Personal Data Protection Act is amended, or if any additional details are announced that explicitly conflict with or contradict this policy, or may result in the Company or related parties being considered in violation of the Personal Data Protection Act, the amended sections of the Act and/or related announcements or regulations shall be enforced in place of such explicitly conflicting or contradictory sections.

14. Penalties

Failure to comply with the Personal Data Protection Policy will result in civil, criminal, and administrative penalties for the Company and the violator, with a maximum penalty of a fine not exceeding 5,000,000 Baht and imprisonment for not more than 1 year. Furthermore, any party involved in the violation of personal data must take responsibility for their actions and face penalties according to the Personal Data Protection Act, B.E. 2562, subject to consideration by the Executive Committee.

15. Policy Review

The Personal Data Protection Policy shall be reviewed and presented to the Board of Directors for approval at least once a year.

This Personal Data Protection Policy was reviewed and approved by the Board of Directors at Meeting No. 8/2025 on November 11, 2025.

Announced on November 25, 2025.

(Mr. Siwaphong Boonsalee)

Managing Director