018/2567

10 January 2024

Saksiam Leasing Public Company Limited
Privacy Notice

Saksiam Leasing Public Company Limited and its subsidiaries ("the Group Companies") deeply value the privacy of our customers. This Privacy Notice is hereby established to inform our customers of the Company's policies regarding the collection, use, and disclosure of personal data of natural persons ("you"), in strict compliance with the Personal Data Protection Act B.E. 2562 ("PDPA"), as well as all relevant laws and regulatory rules. The Company has issued this Privacy Notice for applicants and personnel to clarify the details, management methods, and processing of personal data that the Company receives from you. This includes stating the purposes of collection, use, disclosure, and transmission, as well as the retention period of such personal data and your statutory rights as a data subject, with details set forth as follows:

Section 1: Definitions

The Company: Saksiam Leasing Public Company Limited.

Subsidiary: Saksiam Maker Drone Company Limited.

You: Customers, employees, former employees, directors, executives, shareholders, job applicants, and any other natural persons associated with the Company's personnel.

Personal Data: Any information relating to a natural person, which enables the identification of such person, whether directly or indirectly, but excluding the data of a deceased person specifically.

Sensitive Personal Data: Personal data regarding race, ethnicity, political opinions, cult, religious or philosophical beliefs, sexual behavior, criminal records, health data, disability, trade union information, genetic data, biometric data, or any other data which affects the data subject in a similar manner, as announced and specified by the Personal Data Protection Committee.

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.

Personal Data Protection Law: The Personal Data Protection Act B.E. 2562 and its relevant subordinate legislation, including any future amendments thereto.

Section 2: Channels and Sources of Personal Data

The Company collects, uses, or discloses your personal data through various channels as follows:

2.1 Personal Data provided directly to the Company: You may provide personal data directly to the Company. However, in certain cases, the Company may obtain your

personal data from other sources in compliance with the provisions of the PDPA. Personal data collected from other sources may include, but is not limited to:

a) Data received from companies within the Company's financial business group, business partners, and/or any other entities with which the Company maintains legal relations.
b) Data received from persons associated with you (e.g., your family, friends, or recommenders).
c) Data received from corporate customers, in your capacity as a director, authorized representative, agent, assignee, or contact person.
d) Data received from insurance companies and/or any other persons related to insurance policies or insurance claims.

In the event that you provide personal data of other individuals to the Company for executing transactions or any other purposes, you must notify such individuals of the details concerning the collection, use, and disclosure of their personal data, as well as their rights under this Privacy Notice.

2.2 Personal Data collected automatically: The Company may receive your personal data automatically, such as video images recorded via Closed-circuit television (CCTV), or the automatic collection of technical data, activities, visit patterns, and browsing histories using cookies and other similar technologies. You may study further details in the Company's "Cookies Notice".

2.3 Personal Data received from third parties: The Company may receive your personal data from third parties from time to time, such as job search websites, recruitment agencies, and reference persons.

Section 3: Collected, Used, or Disclosed Personal

DataThe personal data collected by the Company under this Privacy Notice is categorized by data subject types as follows: The types of personal data collected, used, or disclosed vary depending on the scope of products and/or services you may have used or expressed interest in, encompassing both general personal data and sensitive personal data, including but not limited to the following:

3.1 General Personal Details: Personal information: Name-surname, National Identification Number, address, telephone number, email, date of birth, age, place of birth, gender, marital status, nationality, educational background, work history, training records, job position, workplace, wage rate, height, weight, photographs, copies of documents for applicant screening, copies of educational qualifications, copies of training certificates (if any), copies of employment certificates or the latest salary slip (if any), and interview evaluations. Contact information: Address, telephone number, and email. Financial information: Bank account details. Data obtained from automated systems or devices: IP Address, cookies, service and

platform usage behaviors, transaction history, voice recordings, photographs, moving images, social media account names, chat logs, and geolocation data.

3.2 Sensitive Personal Details: Data regarding race, religion, disability status, blood group, weight (kg), height (cm), health records, fingerprint data, and criminal records. Other documents include resumes, Curriculum Vitae (CV), or any other information provided to the Company.

3.3 The Company' s Customers: Natural person customers: Existing and current customers of the Company who are natural persons. Corporate customers: Directors, shareholders, ultimate beneficial owners, employees, guarantors, security providers, and legal representatives of past and present corporate customers, including other natural persons with authority to act on behalf of corporate customers. The Company advises corporate customers to ensure that their authorized persons or any related natural persons acknowledge this Privacy Notice.

3.4 Non- Customer Individuals: This includes natural persons who do not hold products or services with the Company but whose personal data must be collected, used, or disclosed. Examples include investors, persons who pay/ transfer funds to or receive funds from the Company's customers, visitors to the Company's website, applications, branches, or offices, guarantors, security providers, ultimate beneficial owners, directors or legal representatives of companies utilizing the Company's services, debtors or lessees of the Company's customers, professional advisors, as well as directors, investors, shareholders of the Company, legal representatives of such persons, and any individuals involved in transactions with the Company or its customers.

Please be informed that links appearing on the Company's platform may redirect you to third-party platforms. Once you enter a third-party platform, the processing of your personal data shall be entirely governed by that third party's privacy policy. The Company highly recommends that you read and understand the privacy policy of such third parties upon accessing their platforms.

3.5 For Job Applicants: Personal details such as name, surname, nickname, address, telephone number, email, date of birth, age, place of birth, gender, marital status, National Identification Number, nationality, educational background, work history, training records, wage rate, height, weight, photographs, copies of documents for applicant screening, copies of educational qualifications, copies of training certificates (if any), copies of employment certificates or the latest salary slip (if any), and interview evaluations.

3.6 For Employee Guarantors: Personal details such as name, surname, nickname, address, date of birth, National Identification Number, card expiration date, blood group, nationality, photographs, telephone number, email, workplace, position,

employment/ salary certificate, and copies of civil servant/ state enterprise identification cards.

3.7 For Student Interns: Personal details such as name, surname, nickname, photographs, date of birth, age, religion, National Identification Number, address, telephone number, email, Line ID, educational history, transcripts, resumes, Curriculum Vitae (CV), official student internship letters from universities, or any other data provided to the Company.

3.8 For Employees and Company Personnel:

3.8.1 General personal details: Name, surname, address, telephone number, date of birth, age, place of birth, gender, marital status, National Identification Number, nationality, educational background, work history, wage rate, height, weight, photographs, and military service status.

3.8.2 Sensitive personal data: Health records, fingerprint data, and criminal records.

3.8.3 Employment-related data: Job position, department, employment start date, termination date, employee ID, years of service, wages and compensation, tax-related information, tax deduction items, performance potential assessments, attendance records, leaves and absences, overtime records, training histories, resignation letters, reasons for resignation, probation evaluations, performance appraisals, promotions, appointments, transfers, change of positions, disciplinary actions, salary certificates, and salary garnishment orders.

3.8.4 Welfare and benefits data: Provident fund, social security, workmen' s compensation fund, group insurance, medical certificates, medical expense claims, receipts, and invoices.

3.8.5 HR management documents: Copies of National Identification Cards, copies of passports (for foreigners), copies of Work Permits, copies of Visas (for foreigners), copies of House Registrations, copies of educational certificates, copies of name/ surname change certificates (if any), copies of training certificates (if any), copies of employment certificates or latest salary slips (if any), copies of military exemption documents (Sor Dor 8, Sor Dor 10), copies of driver's licenses (specifically for drivers), copies of vehicle registrations, and copies of bank book front pages.

3.8.6 Other relevant data: CCTV recordings, including assets associated with you (e.g., vehicles) when entering the Company's premises, buildings, or areas; still or moving images recorded from participating in activities or used for public relations on the Company's website or social media channels; check- in coordinates or location data for attendance tracking; Student Loan Fund (SLF) data; or any other information previously given to the Company, such as application forms.

3.9 For Shareholders: Personal details such as profile history, name, photographs, date of birth, age, religion, Tax Identification Number, National Identification Number, address, telephone number, email, Line ID, nationality, occupation, marital status, passport number, blood group, moving images, bank accounts, number of shares held, and signatures.

3.10 For Nominated Directors: For individuals nominated as directors or associated persons as defined by law, the Company collects personal data directly from you or through other channels, such as government agencies, regulatory bodies, publicly disclosed information, or persons legally authorized to disclose your personal data, as follows:

3.10.1 In the recruitment process: We collect publicly disclosed information or data from persons legally entitled to disclose your data, such as name, surname, gender, photographs, age, educational background, occupation, work history, and directorships or positions held in other companies or enterprises.

3.10.2 For individuals holding directorships: We collect personal data from National Identification Cards or government-issued identity documents, such as name, surname, gender, Identification Number, passport number, photographs, date of birth, age, nationality, religion, place of birth, and height. We also collect other personal data, including training records, activities, marital status, legally connected persons, personal preferences, blood group, address, telephone number, email, contact channels, bank account numbers, vehicle registration, work histories, directorships or positions in other companies, board/sub-committee/shareholder meeting attendance records, director remuneration, securities holding data, names of securities firms, director performance appraisals, and other data mandated by law or Good Corporate Governance principles.

3.11 For Third Parties: The Company may receive personal data of third parties associated with you, such as former supervisors, spouses, family members, internal company contacts, emergency contacts, reference persons, university advisors, or welfare beneficiaries. You must obtain prior consent from these individuals and inform them of the processing of their personal data under this policy before providing their information (e.g., name, surname, contact details, copies of identity documents) to the Company for welfare allocation purposes. If it is necessary to collect Sensitive Personal Data, the Company shall implement appropriate security measures and obtain your explicit consent prior to collection, unless statutory exemptions apply under personal data protection laws, such as labor protection, social security, vital interest prevention, public health public interest, or compliance with legal claims and obligations.

Section 4: Purposes and Legal Bases for Collection, Use, and Disclosure

The Company processes your personal data for the following specified purposes and under the following legal bases:

4.1 For the Company's Customers:

4.1.1 For loan application review and credit consideration.

4.1.2 To perform duties of the Data Controller under credit contracts or loan-related documents.

4.1.3 For internal operational purposes, such as audits, data analysis, credit-related database storage, market research, insurance arrangements, sales promotions, database compilation to offer personalized benefits, or analyzing and presenting products and services of the Data Controller, its agents, or associated parties.

4.1.4 To verify accuracy and/or process payments according to credit contracts or loan-related documents.

4.1.5 To facilitate or perform necessary verification pursuant to credit contracts or loan-related documents.

4.1.6 For debtor credit scoring and analysis.

4.1.7 For debt collection and monitoring.

4.1.8 For detecting, preventing, and prosecuting criminal offenses.

4.1.9 To achieve archiving purposes for public interest, historical research, or statistics, backed by appropriate safeguards to protect data subject rights and freedoms as prescribed by law.

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

4.1.11 Necessary 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 entering into a contract.

4.1.12 Necessary for the performance of a task carried out in the public interest by the Data Controller.

4.1.13 Necessary for the legitimate interests of the Data Controller, or to comply with laws and regulations applicable to the Data Controller.

4.1.14 For other purposes specified within the consent form for personal data collection, use, and disclosure.

4.2 For Suppliers or External Third Parties:

4.2.1 For procurement/sourcing benefits based on the Data Controller's criteria.

4.2.2 For database compilation and utilizing data for internal resource management.

4.2.3 For detecting, preventing, and prosecuting criminal offenses.

4.2.4 To achieve archiving purposes for public interest, historical research, or statistics, backed by appropriate safeguards.

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

4.2.6 Necessary 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 entering into a contract.

4.2.7 Necessary for the performance of a task carried out in the public interest by the Data Controller.

4.2.8 Necessary for the legitimate interests of the Data Controller, or to comply with laws and regulations applicable to the Data Controller.

4.2.9 For other purposes specified within the consent form for personal data collection, use, and disclosure.

4.3 For Job Applicants:

4.3.1 Contract: To enable the Company to operate business according to objectives, such as communicating for appointments, conducting job interviews, verifying applicants' suitability or qualifications for employment, and evaluating/offering other alternative suitable positions.

4.3.2 Legitimate Interest: For necessary operations within the scope that a data subject can reasonably expect, such as CCTV recording, checking applicant qualifications, and verifying identity documents.

4.3.3 Vital Interest / Public Health Interest: To prevent or suppress a danger to a person's life, body, or health, such as emergency contacts and controlling/preventing communicable diseases or pandemics.

4.3.4 Consent: Applied when the Company cannot rely on the aforementioned statutory exemptions or legal bases. The Company will request specific consent from you, processing data strictly according to notified and approved purposes. In processing Sensitive Personal Data, the Company shall obtain explicit consent or proceed as legally permitted, regarding details such as health conditions, criminal history, or COVID-19 test results.

4.4 For Employee Guarantors:

4.4.1 Contract: To enable the Company to operate business according to objectives. When you wish to execute a guarantee contract with the Company, you must provide personal data so the Company can evaluate your qualifications as a guarantor and maintain evidence to establish legal claims. Failure to provide such data prevents the Company from executing the guarantee contract with you.

4.4.2 Legitimate Interest: For necessary operations within the scope that a data subject can reasonably expect, such as CCTV recording. The Company may utilize your personal data for internal management, corporate reporting, working standard management, risk management, and internal audits.

4.4.3 Vital Interest / Public Health Interest: For emergency contacts and managing/preventing communicable diseases or pandemics.

4.4.4 Consent: Requesting explicit consent when statutory legal bases are unavailable, specifically for processing Sensitive Personal Data like health info, criminal history, or COVID-19 test results.

4.5 For Student Interns:

4.5.1 Contract: For appointment communications, interviews, verifying intern qualifications, entering into or performing internship agreements, or administering disciplinary warnings/penalties.

4.5.2 Legitimate Interest: For CCTV recording, verifying intern identities, human resource management, expense reimbursements, welfare/ benefit allocation, organizing seminars, facilities management, and training.

4.5.3 Vital Interest / Public Health Interest: For emergency contacts and managing/preventing communicable diseases or pandemics.

4.5.4 Consent: Requesting specific consent from you when other statutory exemptions are unavailable, particularly for Sensitive Personal Data.

4.6 For Employees and Personnel:

4.6.1 Contract: Necessary for contract performance where you are a party, or for processing steps at your request prior to entering into an agreement, ensuring smooth business operations. This includes employment hiring, employee registration, executing employment guarantee letters, training, interview/performance appraisals, attendance tracking, leave tracking, wage payments, tax administration, disciplinary actions, issuing certificates, welfare management, health and safety management (e.g., annual physical check- ups, vaccinations, health insurance) , resignation management, retirement, and termination. This includes using and disclosing names, surnames, and personal data appearing in identity document copies of directors or personnel to verify identity as an authorized representative of the Company strictly for signing contracts, documents, registrations, power of attorney, or executing any transactions on behalf of the Company, as well as using and disclosing names in Company announcements, forms, or documents for business operations.

4.6.2 Legal Obligation: For labor protection, social security, national health security, and statutory medical welfare. This encompasses complying with corporate laws or lawful orders, such as Labor Protection Law, Labor Relations Law, Social Security Law, Occupational Health, Safety, and Working Environment Law, Tax Law, salary garnishments via the Legal Execution Department, Student Loan Fund (SLF) management, employee

registration rosters, withholding tax payments, establishing the Labor Welfare Committee, or other business litigation.

4.6.3 Legitimate Interest: For necessary operations within reasonable expectations, such as CCTV recording, personnel management, expense processing, welfare allocation, provident fund membership, organizing events/seminars, facilities provisioning, skill/capability training, and parking sticker management.

4.6.4 Necessary for the establishment, compliance, exercise, or defense of legal claims.

4.6.5 Vital Interest / Public Health Interest: For emergency contacts and managing/preventing communicable diseases or pandemics.

4.6.6 Consent: Requesting specific consent when legal exemptions are inapplicable. In processing Sensitive Personal Data (e.g., physical exam data, biometric fingerprints, criminal records), the Company proceeds as legally mandated or upon receiving explicit consent. Note: Data processing relevant to contract performance or legal obligations is strictly necessary to achieve those purposes. If you choose not to provide such personal data, it may cause legal non-compliance, or prevent the Company from delivering services, executing contracts, or performing contractual duties toward you. If the Company utilizes data for unlisted purposes, an additional Privacy Notice will be provided to explain such usage before processing.

4.7 For Shareholders and Company Directors:

4.7.1 Contract: Necessary to perform contracts where you are a party or to take steps at your request prior to entering into an agreement.

4.7.2 Legal Obligation: For company administration (e.g., incorporation, capital increase, capital reduction, corporate restructuring, registration changes), shareholder meetings, director recruitment and appointments, board meetings, shareholder rights/ dividend management, accounting and statutory audit reports, and transmitting mandatory corporate documents under public limited company and stock exchange laws.

4.7.3 Legitimate Interest: For company administration, recording meeting video/ audio, security management, organizing shareholder activities, transmitting shareholder updates, or establishing legal claims.

4.7.4 Vital Interest / Public Health Interest: For emergency contacts and managing/preventing communicable diseases or pandemics.

4.7.5 Consent: Utilizing personal or sensitive data via explicit consent when other statutory bases are legally unavailable.

Section 5: Your Legal Rights

The PDPA aims to give you greater control over your personal data. You may exercise your rights through the Company's designated channels as follows:

- **5.1 Right of Access and Obtaining Copies:** You have the right to access and obtain a copy of your personal data held by the Company, unless the Company is legally or judicially entitled to reject your request, or if your request impacts and damages the rights and freedoms of others.
- **5.2 Right to Rectification:** You have the right to request the Company to correct or update inaccurate or incomplete personal data.
- **5.3 Right to Erasure / Deletion:** You have the right to request the Company to erase, destroy, or anonymize your data, unless the Company maintains legitimate legal grounds to reject your request.
- **5.4 Right to Restriction of Processing:** You have the right to request the Company to restrict data usage in certain cases (e.g., during rectification or objection verifications, or when you request restriction instead of erasure for data no longer needed because you require its preservation to establish, comply, or defend legal claims).
- **5.5 Right to Object:** You have the right to object to the collection, use, or disclosure of data processed under Legitimate Interest or for direct marketing, unless the Company holds overriding legitimate grounds (e.g., demonstrating that collection holds higher legal grounds, or is for establishing legal claims or public interests).
- **5.6 Right to Data Portability:** You have the right to receive your personal data in a format readable or usable by automated tools/devices, and request automated transmission to a third party, unless technically unfeasible or legally restricted.
- **5.7 Right to Withdraw Consent:** You have the right to withdraw given consent at any time through corporate procedures, unless restricted by nature. Withdrawal does not affect prior lawful processing based on consent given before withdrawal. Marketing consent changes can be adjusted via Section 10 channels or via dpo@saksiam.co.th.
- **5.8 Right to Lodge a Complaint:** You have the right to lodge a complaint with the Personal Data Protection Committee or its office if the Company fails to comply with the PDPA.

Section 6: Disclosure of Personal Data

The Company may disclose your personal data for specified purposes and under legal rules to the following entities and persons:

- **6.1 Internal business units:** Such as human resource personnel, executives, supervisors, accounting departments, and information technology departments.

6.2 **Government agencies and regulatory bodies:** Such as the Social Security Office, the Revenue Department, the Ministry of Labor, the Ministry of Commerce, the Department of Business Development, the Department of Labor Welfare and Protection, the Legal Execution Department, the Department of Skill Development, banks, and asset management companies. This includes entities legally authorized to request disclosure, such as the Anti-Money Laundering Office (AMLO), the National Anti-Corruption Commission (NACC), the Royal Thai Police, the Department of Special Investigation (DSI), the Office of the Attorney General, and the Courts.

6.3 **External units:** Such as external training institutes, hospitals, insurance companies (for company welfare), external auditors, customers, or other relevant entities. When disclosing data to third parties, the Company shall implement appropriate protection measures complying with personal data protection standards. For cross-border data transfers, the Company ensures that destination countries, international organizations, or overseas recipients maintain adequate data protection standards. In certain cases, explicit transfer consent will be requested as required by law.

Section 7: Personal Data Retention Period

The Company retains personal data for the duration necessary to fulfill purposes or as mandated by law, as follows, after which the data shall be deleted or destroyed:

7.1 **Non-selected job applicants:** Retained for a period of 1 year after the screening process is completed.

7.2 **Employees and personnel:** Retained throughout the duration of the employment contract, and continuously stored for a period of 5 years from the termination date of employment, or as mandated by other laws. Data may be stored further for audit purposes during legal dispute statutes of limitation, which extend up to 10 years.

Section 8: Security of Personal Data

The Company utilizes data storage systems equipped with appropriate mechanisms, techniques, and legal security measures to restrict access strictly to relevant employees and staff, preventing unauthorized use, disclosure, destruction, or access.

Section 9: Data Subject Rights Implementation

As a data subject, you hold legal rights under the PDPA. To exercise your rights, you may submit a request via the "Data Subject Right Request Form" by contacting the Company through the contact details provided in Section 10:

9.1 Right to Withdraw Consent: You can withdraw consent at any time during data retention, unless restricted by law or favorable contracts. The Company will inform you of the potential impacts of withdrawal.

9.2 Right of Access: You may request access to or copies of your personal data under Company responsibility, including requesting disclosure of unconsented data sources. Requests can be denied if they impact the rights and freedoms of others, or if you lack legal access rights.

9.3 Right to Data Portability: Requesting data transmission to another data controller.

9.4 Right to Object: Objecting to collection, use, or disclosure at any time for direct marketing, scientific research, or statistics. Requests can be denied for public interest tasks or overriding legitimate legal grounds.

9.5 Right to Erasure / Deletion: Requesting deletion or anonymization if data processing is believed unlawful, unnecessary under policy purposes, or when consent is withdrawn/objected. Requests can be denied if legal retention timelines apply or if data is required for operations.

9.6 Right to Restriction of Processing: Requesting temporary restriction during rectification/ objection audits, or when preserving data instead of erasing it to establish legal claims.

9.7 Right to Rectification: Rectifying data to be accurate, current, complete, and free from misconceptions.

9.8 Right to Lodge a Complaint: Lodging complaints with the Office of the Personal Data Protection Committee for corporate violations.

Section 10: Contact Information

For any questions regarding this Privacy Notice, you may contact the Company using the following details:

Data Controller Details:

Name-Surname: Mr. Phitak Takham, Personal Data Protection Officer (DPO)

Address: No. 49/47 Chetsadabodin Road, Tha It Sub-district, Mueang Uttaradit District, Uttaradit Province 53000

Telephone: 088-776-4049

Email: dpo@saksiam.co.th

Section 11: Changes to this Privacy Notice

The Company may update this Privacy Notice from time to time to align with changes in data processing methods and amendments to personal data protection laws or other related legislation. The Company will notify you of any material changes through appropriate channels.

Announced on January 10, 2024.

(Mr. Siwaphong Boonsalee)

Managing Director