

Privacy Notice

AIRA Property Public Company Limited.

AIRA Property Public Company Limited. (the “Company”) recognizes the importance of personal data protection and is committed to ensuring that the governance and management of personal data are conducted in compliance with applicable personal data protection laws and other relevant laws and regulations. Accordingly, the Company would like to provide you with the following information in accordance with the Personal Data Protection Act B.E. 2562 (2019) (the “PDPA”), the key details of which are set forth below:

1. Definitions

“Company”	means AIRA Property Public Company Limited, acting as the Data Controller.
“You”	means a natural person who is the owner of Personal Data.
“Personal Data”	means any information relating to a natural person that enables such person to be identified, whether directly or indirectly, such as first and last name, age, address, telephone number, identification card number, financial information, and other similar information. This does not include the Personal Data of a deceased person.
“Sensitive Personal Data”	means Personal Data pertaining to racial or ethnic origin, religious or philosophical beliefs, political opinions, sexual behavior, criminal records, health information, disabilities, trade union information, genetic data, biometric data, such as fingerprint scanning and facial recognition, or any other data which may similarly affect the Data Subject, as prescribed by the Personal Data Protection Committee.
“AIRA Property Group”	means AIRA Property Public Company Limited and any company in which AIRA Property Public Company Limited directly or indirectly holds shares, or over which AIRA Property Public Company Limited has management control pursuant to applicable laws or the articles of association of such company.

“AIRA Capital Group”

means AIRA Capital Public Company Limited and any company in which AIRA Capital Public Company Limited directly or indirectly holds shares, or over which AIRA Capital Public Company Limited has management control pursuant to applicable laws or the articles of association of such company.

“Shareholder”

means a natural person whose name is registered as a shareholder of the Company according to the Company’s shareholder register, including any shareholder’s appointed representative or any person having rights under applicable laws.

“Representative”

means a natural person who is appointed or authorized to act, contact, coordinate, or perform any act on behalf of a Shareholder, Director, Sub-committee Member, Executive, Employee, or any other person related to the Company.

“Director”

means a natural person who has been appointed to serve as a director of the Company pursuant to applicable laws, the Company’s articles of association, or a resolution of the Company’s authorized person or body.

“Sub – committee”

means a natural person who has been appointed to serve as a member of any committee, working committee, or sub-committee established by the Company to consider, review, supervise, oversee, or undertake any matter as assigned.

“Executive”

means a natural person holding an executive position within the Company with authority and responsibility for management, policy-making, decision-making, or supervision of the Company’s operations in accordance with the Company’s organizational structure or as otherwise determined by the Company.

“Employee”

means a natural person who is employed or appointed to work for the Company, whether as a permanent employee, temporary employee, contractual employee, or any other

“Job Applicant”	means a natural person who applies for employment with, or expresses an intention to apply for employment with, the Company, whether directly, through a recruitment agency, or through any other channel designated by the Company, including a person who is undergoing the selection or consideration process for employment with the Company.
“Business Partners, Customers, and Suppliers”	means natural persons, juristic persons, or other organizations that have a business relationship with or provide services to the Company, including contractors, service providers, vendors, consultants, outsourced service providers, subcontractors, and business partners, as well as natural persons associated with or representatives of such persons or juristic persons.
“Personal Data Protection Coordinator”	means a person appointed by the Company to coordinate, support, and monitor the Company’s personal data protection activities to ensure compliance with applicable laws, policies, regulations, and guidelines, including coordinating with relevant authorities and persons in matters relating to personal data protection as assigned.
“PDPC”	means Personal Data Protection Committee Office.

2. Personal Data Collected

The Company may collect Personal Data of various categories of individuals who are involved in or have a relationship with the Company’s business operations, including but not limited to Shareholders, Directors, Executives, Employees, Job Applicants, Business Partners, contractors, tenants, service users, visitors, activity participants, and other individuals who have a relationship with or are otherwise involved in the Company’s business operations. The types of Personal Data collected may vary depending on the nature of the relationship, the purposes of processing, and the relevant services, as set out below:

General Personal Data

- (a) Personal information, such as first and last name, date and place of birth, marital status, photographs, signature, information appearing on an identification card, passport, or other official documents, including identification card number. The Company will collect such information only to the extent necessary and for lawful purposes.
- (b) Contact information, such as address, telephone number, email address, LINE ID, social media contact information, and workplace address.
- (c) Security-related information, such as images captured by closed-circuit television (CCTV), as well as information identifying an individual's property, such as vehicle information and vehicle registration number, in connection with access to the Company's premises.
- (d) Employment and professional information, such as job title, directorship position, executive position, department or organization where you work, nationality, educational background, employment history, training courses attended, test results, competencies, and assessments of behavior, attitude, and suitability for performing work.
- (e) Financial information, such as bank account number, financial transaction information, securities or shareholding information, and tax-related documents relating to transactions between you and the Company.
- (f) Information relating to access to and use of electronic systems associated with the Company, such as email address, Internet Protocol (IP) address, browser type, computer traffic data (log files), cookies, and chat history on applications, as well as comments or references concerning the Company or its business made on the Internet or through other channels.
- (g) Information provided by you when you contact or participate in any activities with the Company, including photographs, video recordings, and audio recordings for public relations, event management, or other purposes related to the Company's business operations.

Sensitive Personal Data

- (h) Sensitive Personal Data, such as health information, disability information, biometric data, religious information, or other types of Sensitive Personal Data as prescribed by applicable laws.

The Company will collect, use, and disclose Sensitive Personal Data only to the extent necessary and in accordance with the conditions prescribed by applicable laws. The Company will obtain consent from the Data Subject where consent is required by law, except where applicable laws permit the Company to process such Sensitive Personal Data without obtaining consent.

For the purpose of verifying your identity, the Company would like to inform you that, in cases where the Company is required to obtain copies of identification documents, such as an identification card, passport, or other official documents, such documents may contain Sensitive Personal Data, including religious information or blood type. The Company does not intend to collect such Sensitive Personal Data. Therefore, you are requested to cross out or black out such information before submitting the documents to the Company. If you do not do so, the Company will consider that you authorize the Company to redact such information. Such documents shall remain valid and legally

effective in all respects. However, if the Company is unable to redact such information due to certain limitations, the Company confirms that the collection and use of such information will be carried out solely for the purpose of identity verification. The Company does not intend to collect or use any Sensitive Personal Data appearing on such documents beyond what is necessary for such identity verification.

3. Respect for Privacy Rights

The Company respects the privacy rights of Data Subjects and recognizes that Data Subjects have the right to expect the security and protection of their Personal Data. Accordingly, the Company will collect, use, and process your Personal Data only for relevant and specified purposes. The Company has implemented strict measures to maintain the security of Personal Data and to prevent the unauthorized, unlawful, or improper use of Personal Data.

4. Collection of Personal Data

When collecting Personal Data directly from the Data Subject, and when using or disclosing such Personal Data, the Company will obtain consent from the Data Subject before or at the time of collection where consent is required by applicable laws. The Company will process Personal Data only to the extent necessary for the specific and clearly stated purposes communicated by the Company.

The Company may also collect Personal Data from sources other than the Data Subject directly, but only where necessary and in accordance with applicable laws. Such sources may include relevant service providers, publicly available sources, or other lawful sources.

5. Purposes of Collection, Use, and Disclosure of Personal Data

The Company collects, uses, and discloses your Personal Data for the following purposes:

5.1 Personal Data of Shareholders and Representatives

- 5.1.1 To manage and maintain the Company's shareholder register in compliance with the laws governing public limited companies and other applicable laws.
- 5.1.2 To process and make dividend payments to Shareholders, or to receive payments in connection with an increase in the Company's registered capital.
- 5.1.3 To verify and authenticate identity, including verifying the status of Shareholders of the Company, based on relevant documents and information.
- 5.1.4 To facilitate and administer Shareholders' rights, including convening Shareholders' meetings, registering attendance, exercising voting rights, recording photographs, audio, and/or video during meetings, preparing relevant documents, and conducting related communications and coordination.
- 5.1.5 To provide Shareholders with information and updates regarding the Company's activities, as deemed appropriate by the Company.
- 5.1.6 To maintain a stakeholder database and/or use Personal Data for relationship management, internal communications, and coordination relating to the Company's operations.

- 5.1.7 To comply with applicable laws and regulations and to communicate and coordinate with external authorities, such as the Department of Business Development, government agencies, regulatory authorities, and other relevant authorities, including the preparation, maintenance, submission, or disclosure of information and documents as required by law.
- 5.1.8 To provide assistance for law enforcement purposes, investigations conducted by or on behalf of the Company, by police officers, government authorities, or other regulatory authorities in any country or jurisdiction, and to fulfill reporting obligations and other requirements under applicable laws or as otherwise agreed with or required by government authorities or other regulatory authorities in any country or jurisdiction.

5.2 Personal Data of Directors, Sub – committee, and Senior Executives

- 5.2.1 To carry out necessary processes for the consideration and selection of Directors or Senior Executives, including assessment, selection, appointment, and other relevant internal management processes relating to the consideration, selection, and appointment of Directors or Senior Executives.
- 5.2.2 To carry out various activities and transactions between you and the Company, including activities undertaken where you act as a representative of or on behalf of the Company, such as:
- Payment of remuneration to Directors, Sub-committee Members, or Senior Executives, including any necessary activities relating to such remuneration payments;
 - Preparation and maintenance of Personal Data, including profiles and records of Directors, Sub-committee Members, or Senior Executives, for the Company's database and record-keeping purposes;
 - Sending meeting invitations, meeting agendas, supporting documents, and other relevant documents;
 - Nominating you for appointment as a Director or Sub-committee Member of companies within the AIRA Property Group;
 - Disclosing information through the Company's website and/or providing such information to external organizations for purposes such as applications for training programs, courses, awards, or other activities in which you participate in your capacity as a Director, Sub-committee Member, or Senior Executive;
 - Disclosing information, such as biography, first and last name, age, educational background, employment history, and directorship positions, through various media, including printed media, advertising media, electronic media, websites, and other channels, for access, acknowledgment, and further dissemination by third parties;

- Collecting, using, and/or disclosing Personal Data of Directors, Sub-committee Members, and Senior Executives for the Company's business operations and management, including as supporting evidence for the Company's transactions;
- Disclosing Personal Data and verifying the accuracy of relevant information (Know Your Customer: KYC) in connection with transactions with domestic and overseas banks;
- Disclosing and reporting information concerning Directors, Sub-committee Members, and Senior Executives to relevant regulatory authorities;
- Disclosing necessary information for compliance with various assessment criteria or evaluation programs in which the Company participates.

5.2.3 To use the information for applying for access to electronic systems or for granting access rights to and/or use of the Internet or various electronic systems.

5.2.4 To comply with applicable laws and to communicate and coordinate with the Department of Business Development, government agencies, regulatory authorities, financial institutions, and other relevant external organizations, including the preparation, maintenance, submission, or disclosure of information and documents as required by applicable laws or such authorities or organizations.

5.2.5 To establish legal claims, grant and receive powers of attorney, comply with or exercise legal claims, defend against legal claims, conduct legal proceedings, and undertake enforcement proceedings in accordance with applicable laws.

5.2.6 To collect and use your Personal Data, including your name, surname, position, photographs, and video recordings, where you participate in meetings, activities, or other events related to the Company, for public relations and communications through various channels, such as the Company's website, internal email, printed media, or other online media.

5.2.7 To provide assistance for law enforcement purposes, investigations conducted by or on behalf of the Company by police officers, government authorities, or other regulatory authorities in any country or jurisdiction, and to fulfill reporting obligations and other requirements under applicable laws or as otherwise agreed with or required by government authorities or other regulatory authorities in any country or jurisdiction.

5.3 Personal Data of Employees and Job Applicants

5.3.1 To manage human resources, including assisting employees in adapting to new roles (onboarding), planning and carrying out employee recruitment, evaluating job applications for new employment opportunities and making employment decisions, providing training, evaluating promotions, career advancement, transfers, assignments to other locations, workforce planning, performance evaluations, internal reporting, data analysis, and other employment-related management activities.

- 5.3.2 To verify and authenticate the identity of Employees, control and monitor access to and exit from the Company's premises, and record attendance and working hours using biometric data through the facial recognition system, in accordance with the systems and measures prescribed by the Company.
- 5.3.3 To verify or identify the identity of Employees when accessing digital technology systems and to monitor Employees' use of such digital technology systems in accordance with the Company's Information Technology System User Policy.
- 5.3.4 To comply with applicable legal processes, laws, rules, and regulations, including court orders, and to fulfill requirements under applicable laws, rules, regulations, agreements, or policies established by government regulatory authorities, law enforcement agencies, government authorities, dispute resolution bodies, or authorities responsible for regulating the Company's business, whether domestic or foreign.
- 5.3.5 To administer and comply with requirements relating to salaries, compensation, benefits, compensation plans, future employment offers, awards, and compensation records.
- 5.3.6 To facilitate internal communications and communicate appointments or arrangements to individuals both within and outside the Company, whether by telephone, text messages, email, postal mail, electronic media, applications, or any other communication channels, for the purpose of communicating relevant information to Employees.
- 5.3.7 To conduct surveys, provide information for government statistical purposes, or respond to any government forms or requests, for any lawful purpose.
- 5.3.8 To verify your information as required by applicable laws, including physical information or your ability to perform work, and to assess and promote equal employment opportunities.
- 5.3.9 To investigate complaints and allegations of inappropriate conduct or misconduct, or as part of the Company's disciplinary process.
- 5.3.10 To maintain employee records, arrange insurance, and manage medical records and insurance plans.
- 5.3.11 To conduct reference and background checks of Employees or other individuals, identify and prevent conflicts of interest or potential conflicts of interest, comply with applicable requirements, regulations, or orders of administrative authorities in or outside your country, and verify employment agreements entered into by any member of the Company.
- 5.3.12 To support investigations conducted by competent law enforcement officers and to provide assistance for law enforcement purposes, including investigations conducted by or on behalf of the Company by police officers, government authorities, or other regulatory authorities in any country or jurisdiction, and to fulfill reporting obligations

and other requirements under applicable laws or as otherwise agreed with or required by government authorities or other regulatory authorities in any country or jurisdiction.

5.3.13 To maintain the security of the Company, including investigating, preventing, or taking action in relation to violations of applicable laws, mitigating risks where there are reasonable grounds to suspect fraud, money laundering, threats to national security, unlawful activities, or activities reasonably believed to be unlawful, or circumstances that may affect the safety, health, or physical well-being of other individuals.

5.3.14 For purposes of corporate restructuring and corporate transactions that may result in the transfer or disclosure of your Personal Data as part of a sale or acquisition of a business, or as part of an offer to purchase or sell a business.

5.3.15 To comply with the requirements under the Company's applicable internal policies and procedures.

5.3.16 To store, record, back up, or securely dispose of Personal Data.

5.3.17 To carry out general administrative activities relating to the purposes set out above and to undertake other necessary activities that are directly related to any of the foregoing purposes.

5.4 Personal Data of Business Partners, Customers, and Suppliers

5.4.1 To communicate with you, establish a business relationship, verify your identity, and verify the accuracy of any information provided by you to the Company.

5.4.2 To offer, sell, provide, manage, and process products and services, including carrying out procurement and purchasing procedures, communicating with you regarding your orders, fulfilling and delivering your orders, and providing services to you.

5.4.3 To perform or enter into a contract between you and the Company, including carrying out procedures, managing, completing, and giving effect to any requests or transactions specified in this Privacy Notice or any other documents that you may provide to the Company from time to time; assessing risks that may affect the Company's business operations; collecting outstanding payments from you; amending or terminating contracts; following up on and collecting debts; and enforcing legal remedies relating to products or services.

5.4.4 Where you are a supplier or its representative, to receive products or services from you, exercise any rights under the contract between you and the Company, obtain information regarding products and/or services, receive support or assistance in managing products and/or services, or contact you in response to any inquiries.

5.4.5 To communicate with you, including providing information regarding management matters and other information relating to products or accounts that you may have with the Company, providing technical support relating to the Company's websites and applications, and communicating any changes that may be made to this Privacy Notice in the future.

- 5.4.6 To process payment information, issue invoices, collect or make payments, confirm orders, and for accounting, financial management, and auditing purposes of the Company.
- 5.4.7 To investigate, prevent, or take action in relation to violations of applicable laws; mitigate risks where there are reasonable grounds to suspect fraud or deception, money laundering, threats to national security, unlawful activities, or activities reasonably believed to be unlawful, or circumstances that may affect the life or physical safety of other individuals.
- 5.4.8 To provide information about other products or services that the Company considers may be of interest to distributors, suppliers, or their representatives. Distributors, suppliers, or their representatives may notify the Company at any time if they do not wish to receive such information.
- 5.4.9 To maintain the security of the Company.
- 5.4.10 To support the Company's business operations, including communication, statistical analysis, information system management, testing, development, and maintaining systems and security control measures.
- 5.4.11 For purposes of corporate restructuring and corporate transactions that may result in the transfer or disclosure of your Personal Data as part of a sale or acquisition of a business, or as part of an offer to purchase or sell a business.
- 5.4.12 To comply with applicable regulations and requirements and to conduct audits of the Company's business operations, including both internal and external audits.
- 5.4.13 To comply with the requirements under the Company's applicable internal policies and procedures.
- 5.4.14 To store, record, back up, or securely dispose of Personal Data.
- 5.4.15 To comply with applicable laws, rules, regulations, agreements, or policies established by government regulatory authorities, law enforcement agencies, government authorities, dispute resolution bodies, or authorities responsible for regulating the Company's business, whether domestic or foreign.
- 5.4.16 To provide assistance for law enforcement purposes, including investigations conducted by or on behalf of the Company by police officers, government authorities, or other regulatory authorities in any country or jurisdiction, and to fulfill reporting obligations and other requirements under applicable laws or as otherwise agreed with or required by government authorities or other regulatory authorities in any country or jurisdiction.
- 5.4.17 For quality assurance and training purposes where the Company records communications.
- 5.4.18 To carry out general administrative activities relating to the purposes set out above and to undertake other necessary activities that are directly related to any of the foregoing purposes. Where the Company collects your Personal Data for any other purpose, the

Company intends to inform you of such purpose at the time the Personal Data is collected.

In addition to the purposes stated above, the Company may also collect, use, and disclose Personal Data for the purposes of maintaining security and orderly operations, managing health and safety matters, communicating where necessary or in the event of an emergency, controlling and monitoring access to the Company's premises, registering visitors, recording images through closed-circuit television (CCTV), maintaining the security of the Company's information technology systems and the Company's data, as well as protecting the Company's legitimate rights and interests, including preventing or resolving disputes and taking any relevant legal action.

Where the Personal Data collected by the Company for the above purposes is necessary for the performance of a contract or compliance with applicable laws and regulations, failure to provide such necessary Personal Data may result in a violation of applicable laws or may prevent the Company from managing or performing the relevant contract or providing the necessary services or facilities to you.

In the event that the Company subsequently changes the purposes for which Personal Data is collected, used, or disclosed, the Company will notify you of such changes and take any other actions required by applicable laws, including maintaining records of such amendments or additions as evidence.

Furthermore, where you provide the Company with Personal Data of another individual, for example, where you act as a secretary or coordinator for a Data Subject who contacts or communicates with the Company, you are responsible for informing such Data Subject of this Privacy Notice and obtaining the lawful consent of such individual where consent is required by applicable laws. Where necessary, the Company may request documentary evidence that such Data Subject has been duly informed of this Privacy Notice and that the required consent has been properly obtained.

6. Retention Period for Personal Data

The Company will retain your Personal Data for as long as necessary to fulfill the purposes for which such Personal Data is collected, used, and disclosed, as well as for the period required by applicable laws or the applicable statutory limitation period relating to the exercise of legal claims or rights.

Upon expiry of the applicable retention period, the Company will delete, destroy, or anonymize your Personal Data so that it can no longer be used to identify you, unless applicable laws specifically require the Company to retain such Personal Data for a longer period.

7. Data Security

The Company has established and implemented appropriate measures to ensure the security of Personal Data in accordance with the Company's information security policies and guidelines under its Information Security Management System (ISMS), which is certified in accordance with the ISO/IEC 27001 standard. Such measures are designed to prevent the loss, unauthorized access, use, disclosure, destruction, alteration, modification, or unlawful or unauthorized processing of Personal Data.

The Company will regularly review and appropriately update its Personal Data security measures, taking into consideration the nature of the Personal Data, relevant risks, technological developments, and the context of the processing of Personal Data. The Company will also take necessary measures to prevent, detect, and manage incidents that may adversely affect the security of Personal Data.

8. Rights of Data Subjects

Data Subjects have the rights prescribed under the Personal Data Protection Act B.E. 2562 (2019) (the “PDPA”), as follows:

- 8.1 Right to withdraw consent.
- 8.2 Right to request access to Personal Data and obtain a copy of Personal Data, including the right to request disclosure of the source from which the Personal Data was obtained where the Data Subject has not previously provided consent to the Company.
- 8.3 Right to request the transmission or transfer of Personal Data to a third party or to the Data Subject themselves, where such Personal Data can be read or used by an automated tool or equipment.
- 8.4 Right to object to the collection, use, or disclosure of Personal Data.
- 8.5 Right to request the deletion, destruction, or anonymization of their Personal Data so that the Data Subject can no longer be identified.
- 8.6 Right to request the restriction of the use of Personal Data.
- 8.7 Right to request the rectification of Personal Data to ensure that it is accurate, up to date, complete, and not misleading.
- 8.8 Right to lodge a complaint in the event that the Company, including its employees, fails to comply with personal data protection laws.

In the event that a Data Subject submits a request to exercise any of the above rights, the Company will process such request within the period prescribed by law. The Company reserves the right to refuse or not proceed with such request where required by law, or where the Data Subject chooses to provide only certain Personal Data, which may result in the Company being unable to fully carry out certain activities or provide certain services as required.

9. Disclosure of Personal Data to Other Persons or Organizations

The Company may disclose your Personal Data to other persons or organizations with your consent or where such disclosure is permitted by applicable laws. The recipients of such Personal Data will collect, use, and/or disclose your Personal Data within the scope of your consent or the relevant scope specified in this Privacy Notice.

The Company may disclose your Personal Data to other persons or organizations based on your consent or other lawful bases for the purposes specified in this Privacy Notice, such as Personal Data Processors, business partners, external service providers, the Company’s representatives, subcontractors, financial institutions, auditors, external auditors, persons authorized by law, juristic persons or any other persons who have a relationship with or

have entered into a contract with the Company, including executives, employees, contractors, representatives, and consultants of the Company and of such recipients of the Personal Data.

The Company may be required to disclose your Personal Data to other persons or organizations that are strategic partners, both domestically and internationally, who work with the Company in providing products and services in various forms, or as reasonably necessary to enforce the Company's terms and conditions, or in the event of corporate restructuring, merger, or sale of business. Personal Data may also be disclosed to the Company's external assessors, government agencies, or government authorities as required by law, court orders, or orders of authorized officers. Personal Data will be kept confidential, whether in documentary or electronic form, including throughout all stages of data transmission.

In the case of the hotel business, the Company may be required to disclose or transfer Personal Data to hotel operators, reservation system providers, membership system providers, or other relevant service providers, which may be located overseas. The Company will implement appropriate Personal Data protection measures in accordance with applicable laws.

10. Personal Data Protection Coordinator

The Company has appointed a Personal Data Protection Coordinator (PDPA Coordinator) to monitor, oversee, and coordinate the Company's personal data protection activities to ensure compliance with the Personal Data Protection Act B.E. 2562 (2019) and other applicable laws, as well as to serve as a point of contact for Data Subjects in exercising their rights under applicable laws.

11. Contact Information

If you have any questions or require further information regarding the protection of your Personal Data, please contact the Company through the following channels:

Personal Data Protection Coordinator (PDPA Coordinator)

Contact Address: AIRA Property Public Company Limited, 188 Spring Tower, 20th Floor, Units 5–6,
Phaya Thai Road, Thung Phaya Thai, Ratchathewi, Bangkok 10400, Thailand

Tel: 02-108-4319 **Email:** Privacy@airaproperty.co.th

12. Changes to the Personal Data Protection Policy and Guidelines

The Company may revise, update, or amend its Personal Data Protection Policy from time to time, or at least once a year, and/or when there are changes to applicable laws, rules, notifications, or requirements of relevant regulatory authorities, as well as when there are changes to the nature of the Company's business operations or its Personal Data processing activities.

Such revisions, updates, or amendments are intended to ensure that the Company's operations remain appropriate and compliant with applicable laws at all times, and are consistent with the Company's business operations, applicable laws, rules, notifications, and relevant guidelines. The Company will notify you of any such changes through appropriate communication channels of the Company.

Announced on 1st September 2026