

DATA PROTECTION NOTICE

This Data Protection Notice (“**Notice**”) sets out the basis which AiRTS (“**we**”, “**us**”, or “**our**”) may collect, use, disclose or otherwise process personal data in accordance with the Personal Data Protection Act (“**PDPA**”). This Notice applies to personal data in our possession or under our control, including personal data in the possession of organisations which we have engaged to collect, use, disclose or process personal data for our purposes. By engaging with us, whether as a vendor, business partner, customer, or other parties, you acknowledge and consent to the practices outlined below.

1. Personal Data

- 1.1. “**Personal Data**” is data about an individual who can be identified from that data or from that data with other information the organization has or is likely to have access.
- 1.2. The types of personal data we collect may include, but are not limited to:
 - a. Name, gender, date of birth, passport or other personal identification numbers, images, photographs, videos, closed circuit television (CCTV) footage, voice recordings;
 - b. Contact information (e.g., address, phone number, email address);
 - c. Payment information (e.g., bank name, bank branch, bank code and account number, including the name of account holder);
 - d. Biometric information;
 - e. Health information (e.g., medical records or requests); and
 - f. Technical information (e.g., IP address or device identification).

2. Personal Data Protection Principles

- 2.1. **Personal Data Collection:** We will collect your personal data only under the following circumstances:
 - a. Your personal data is voluntarily provided by you, or through an authorized representative appointed by you, after you have been notified of the purpose for the collection and have given written consent for the collection and use of such data; or
 - b. The collection and use of your personal data is permitted or mandated by the PDPA or any other applicable laws.
- 2.2. **Personal Data Collection Methods:** We will collect your personal data in the following ways:
 - a. Directly from you when you submit forms, make inquiries, or provide feedback;

- b. Through interactions with our staff via phone calls, emails, or face-to-face meetings;
- c. Through the capture of images in the form of photographs or videos, including via CCTV cameras within premises or during events; or
- d. From trusted third parties (e.g., business partners, public agencies) with your consent or as permitted by law.

2.3. **Purpose of Data Collection:** We will ensure that your personal data is collected, used, and disclosed solely for specified, legitimate purposes at the time of collection or as permitted by law. It will not be further processed in a manner incompatible with those purposes, unless consent is obtained or mandated by law. These purposes include, but are not limited to:

- a. For vendors/service providers/business partners:
 - i. Conduct due diligence/background checks as mandated by law or internal policies;
 - ii. Evaluate products and services provided to us;
 - iii. Grant security clearance and access to our premises; or
 - iv. Any other purposes reasonably related to any of the above.
- b. For customers:
 - i. Conduct due diligence/background checks as mandated by law or internal policies;
 - ii. Manage and evaluate project tenders;
 - iii. Respond to queries and evaluate products and services provided by us;
 - iv. Grant security clearance and access to our premises; or
 - v. Any other purposes reasonably related to any of the above.
- c. For Others:
 - i. Respond to queries, requests, complaints, and feedback;
 - ii. Evaluate employment applications;
 - iii. Conduct interviews and assess candidate suitability;
 - iv. Provide/obtain staff references and perform background checks;
 - v. Process employment pass, visa applications, and job offers;

- vi. Evaluate scholarship applications and award scholarships;
- vii. Evaluate internship and industrial attachment applications;
- viii. Organize community and charitable events;
- ix. Prevent, detect, and investigate crime, including fraud, money-laundering, and terrorist financing; and manage commercial risks.

2.4. **Consent:** We will obtain consent for the collection, use, and disclosure of personal data and will inform you of the purposes for which your personal data will be used or disclosed. We will also seek consent before collecting additional data or using personal data for new purposes, unless authorized by law or directly related to the original purpose.

2.5. **Disclosure:** We respect your privacy and only disclose personal data to third parties when necessary. This may include:

- a. Service providers who assist in providing products or services on our behalf.
- b. Business partners to enhance the services or products offered to you.
- c. Legal or regulatory authorities as required by law.
- d. Professional advisors, such as accountants or legal consultants, for necessary business support.
- e. In case of a business transaction, such as a merger or acquisition, your data may be transferred to the new entity.

We will ensure that any third parties with whom personal data is shared are obligated to protect the data and use it only for the purposes for which it was disclosed.

2.6. **Accuracy:** Please ensure all personal data submitted to us is complete, accurate, and up to date. Inaccurate, incomplete or outdated data may impact our ability to process requests and/or applications effectively. We will take reasonable steps to ensure that personal data is accurate, complete, and relevant for the purposes for which it is processed.

2.7. **Access, Correction and Withdrawal:** You have the right to access, correct, and withdraw consent for your personal data at any time. Upon your request, we will assess it in accordance with applicable laws and update, correct, or delete your personal data as necessary. All requests will be processed within the legally required timeframes, and we will address any concerns you raise, provided the requests comply with relevant legal requirements.

2.8. **Protection:** We will take reasonable measures to safeguard the personal data it holds or controls by employing a range of technological and physical security measures.

These protections are intended to prevent unauthorized access, use, disclosure, alteration, disposal, or loss of personal data.

Additionally, you are encouraged to take every precaution to protect your Personal Data while online. It is recommended that to use a secure browser, frequently update passwords, create strong passwords using a combination of letters and numbers, and keep their username and password confidential.

- 2.9. **Retention and Disposal:** We will retain your personal data only for as long as necessary for the purpose it was collected, or as required by applicable law. Once the data is no longer needed, we will ensure that it is securely destroyed, anonymized, or disposed of.
- 2.10. **Transfers of Personal Data Outside of Singapore:** We generally does not transfer personal data outside of Singapore. However, if such a transfer is necessary, we will obtain your consent and take appropriate measures to ensure that your personal data remains protected to a standard at least equivalent to that provided under the PDPA. This includes establishing contractual agreements with third parties to whom personal data is transferred, ensuring that reasonable security arrangements are in place to protect the personal data.

3. Your Rights

- 3.1. You have the right to submit a request to our DPO at any time to:
- a. Request access to your personal data we hold;
 - b. Correct, update, or delete any inaccuracies in your personal data after submission;
 - c. Withdraw your consent at any time, without affecting the legality of any processing conducted before the withdrawal, subject to the legal basis for processing;
 - d. Appeals for rejected access, correction and withdrawal requests; or
 - e. Enquiry or provide feedback on our personal data protection policies and procedures.
- 3.2. You can submit the request to our DPO via email (DPO@airts.sg), along with details that will assist in processing the request (e.g., specific records or data you wish to access or correct).
- 3.3. You will receive a response within 7 to 30 days, depending on the complexity of the issue. If more time is required, you will be notified with an updated timeline.

Thank you for your trust in AiRTS. We are committed to protecting your privacy and ensuring that your personal data is handled with the utmost care.