

## Notice of AOT Ground Aviation Services Co., Ltd.

### RE: Policy on the Personal Data Protection

---

Whereas the Personal Data Protection Act B.E. 2562 (2019) (“PDPA”) and the Notification of the Personal Data Protection Commission, RE: Measure on the Security of the Personal Data Controller B.E. 2565(2022) stipulate that the Personal Data Controller has the duty to provide the appropriate security measure in order to prevent loss, access, use, change, or disclosure of Personal Data without authority or unlawfulness. Such security measure must comprise the appropriate organizational measure taking into consideration the level of risk according to the purpose of collection, use, disclosure of Personal Data (including the probability of occurrence including effect from the Personal Data breach. In this regard, the policy and practice of Personal Data protection are deemed as the organizational measure for formulating the internal policy (relating to the principle or guideline of operation of the organization relating to Personal Data protection) and for formulating the role, duty of personnel relating such affair including for imposing the measure on punishment if any personnel violates such organizational policy. Therefore, for the purpose of complying with the Personal Data Protection Act B.E. 2562 (2019), AOT Ground Aviation Services Co., Ltd. (**hereinafter shall be referred to as “Company”**) realizes the importance of the Personal Data and the respect for the right of the Data Subject. In this connection, the Company prepares this Policy on the Personal Data Protection in order that collection, use, disclosure of Personal Data under the Company’s responsibility will be efficient and secured, in addition, the Data Subject’s right and freedom will be protected, there will also be the concrete practice. Moreover, this Policy will notify all stakeholders to acknowledge policy, procedure and purpose of the Company relating to collection, use, disclosure of Personal Data and to notify the rights according to the Personal Data Protection Law for showing the transparency and fairness of the Company in doing activities relating to collection, use, disclosure of Personal Data as specified in this Policy (to ensure that Personal Data received by the Company will be used according to the purpose that has already been notified the Data Subject as stipulated by law) according to the details as follow:

#### 1. In this Policy

“Personal Data” means any information relating to a natural Person, which enables the identification of such Person, whether directly or indirectly, but not including the information of the deceased Persons in particular;

“Sensitive Personal Data” means any Personal Data stipulated in Section 26 of the Personal Data Protection Act B.E. 2562 (2019), which comprise race, ethnicity, political opinion, religion or philosophical beliefs, sexual orientation, criminal record, health and disability information, labour union affiliation, genetic information, biometric information or any other data affecting the Data Subject in similar manner as announced and prescribed by the Personal Data Protection Commission.

“Data Subject” means a natural person being the owner of the Personal Data collected, used, or disclosed by the Company.

“Data Controller” means a Person or a juristic person having the power and duties to make decisions regarding the collection, use, or disclosure of the Personal Data;

“Data Processor” means a Person or a juristic person who operates in relation to the collection, use or disclosure of the Personal Data pursuant to the orders given by or on behalf of a Data Controller, whereby such other operating person or juristic person is not the Data Controller.

“Data Sub-Processor” means a Person or a juristic person who is established or assigned by the external service provider (who is the Company’s Data Processor).

## **2. Collection of Personal Data**

### **2.1 Scope of Collection of Personal Data**

The Company will collect Personal Data (divided into various categories) according to the scope as follows:

#### **2.1.1 Limited Personal Data Collection**

The Company will collect Personal Data having the purpose, scope and lawful and fair procedure. In this connection, the Company will collect Personal Data as necessary for operation under the objective of the Company and as stipulated by law only. However, the Company will notify the Data Subject for clearly acknowledging the purpose and details of collection, use or disclosure of Personal Data, before or while collecting such Personal Data according to the conditions provided by law. However, in case where the collection of Personal Data needs requesting for the consent of the Data Subject, the Company will request for the Data Subject's explicit consent before or while collecting such Personal Data.

In case where the Company has necessity to collect the Sensitive Personal Data according to Section 26 of the Personal Data Protection Act B.E. 2562 (2019), the Company will request for the Data Subject's explicit consent before or while collecting such Sensitive Personal Data. But such consent must not be the condition to receive the service (the request for consent must be clearly distinguishable from the condition to receive the service). In this regard, the statement requesting for consent must be clearly, not ambiguous and easily understandable. However, regarding management of the consent, the Service Users must be able to withdraw their consent as easily as they give such consent.

#### **2.1.2 Source of the Collected Personal Data**

1) The Company will collect Personal Data directly from the Data Subject, for instance, to directly collect Personal Data from the Data Subject who gives his/her Personal Data by himself/herself;

2) The Company will collect Personal Data from usage of the Company's website or electronic service, for instance, data of Log, Cookies, etc.

3) The Company will collect Personal Data from other source not directly from the Data Subject, for instance, searching of Personal Data via website or inquiring from the third person where the Company will notify the Data Subject without delay, not exceeding 30 days as from the day on which the Company collects the Personal Data from such source. In addition, the Company will seek the Data Subject's consent to collect such Personal Data, except it is an exceptional case not required to seek consent or to notify the Data Subject as stipulated by law.

In case where the Data Subject must provide the Personal Data in order to comply with laws or agreement, or it is necessary to provide the Personal Data in order to enter into agreement but the Data Subject fails to provide such data, accordingly, the Data Subject may be unable to take action according to the agreement or to receive service according to such agreement.

4) Regarding the collection of the Personal Data of the minors, the incompetent persons, the quai-incompetent persons, the Company takes into account the protection of such Personal Data according to the rules imposed by the Company not violating any law.

### **2.2 Quality of the Collected Personal Data**

The Company will improve the collected Personal Data to be accurate, updated and without misleading of such Personal Data as a priority. The Company prescribes that it will improve the collected Personal Data every 2 years. In case of necessity and if there is any change of such Personal Data, the Data Subject is requested to notify such change to the Company *via* E-mail: [dpo@aotga.com](mailto:dpo@aotga.com)

### **2.3. Retention Period of Personal Data**

The Company will retain the Personal Data for the period of time as necessary to take action according to the purpose that the Company receives such data. However, in order to meet the legal requirement, the Company may retain such Personal Data for a longer period of time. In this regard, after such retention period lapses, the Company will erase or destroy the Data Subject's Personal Data immediately, except in case where you exercise the right to suspend the usage of his/her Personal Data in place of the erasure or destruction, or it is the exceptional case of the erasure or destruction according to other conditions as stipulated by law, or in case where the dispute or lawsuit occurs, the Company reserves the right to further retain such data until the Data Subject exercises his/her right completely or there is the court's final order or judgement of such dispute or lawsuit.

### **3. Lawful Basis**

The Company will collect the Personal Data for the period of time as necessary according to the lawful purpose having already been notified the Data Subject, before or while collecting the Personal Data only, except the following events, the Company can collect the Personal Data without the consent of the Data Subject:

3.1 It is for the achievement of the purpose relating to the preparation of the historical documents or the archives for public interest, or for the purpose relating to research or statistics, in which the suitable measures to safeguard the Data Subject's rights and freedoms are put in place by the Company;

3.2 It is for preventing or suppressing a danger to a Person's life, body or health;

3.3 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;

3.4 It is necessary for the performance of a task carried out in the public interest, or it is necessary for the exercising of official authority vested in the Company;

3.5 It is necessary for legitimate interests of the Company or any other Persons or juristic persons, except where such interests are overridden by the fundamental rights of the Data Subject of his or her Personal Data; or

3.6 It is necessary for compliance with a law.

However, if the Company has already considered and found that such the Personal Data processing is not under the above-mentioned 6 lawful basis, the Company will request for the Data Subject's consent before or while processing the Personal Data which is under the consent basis.

In regard to the processing of Sensitive Personal Data according to Section 26 of the Personal Data Protection Act B.E. 2562 (2019), if the processing of such Personal Data has no lawful basis as stipulated in Section 26, the Company will request for the Data Subject's explicit consent before or while collecting such Personal Data.

### **4. Request for Consent**

In case where the Company must use the Data Subject's consent as the lawful basis of the Personal Data processing, the Company will request for the Data Subject's consent before or while collecting such Personal Data. The Company will notify the Data Subject of detail where such detail must at least contain the subject matters as follow:

- 1) Purpose of collection of the Personal Data in order to use or disclose it;
- 2) The Personal Data collected by the Company including the period of retention of Personal Data;
- 3) Categories of persons or agencies to which Personal Data may be disclosed;
- 4) Data regarding the Company's Point of Contact;
- 5) Data Subject's rights as stipulated in the Personal Data Protection Act B.E. 2562 (2019)

## **5. Use or Disclosure of the Personal Data**

5.1 The Company will not disclose the Personal Data of the Data Subject other than the purpose of collection of the Personal Data except the action to be taken according to the Court's order or laws, order or relevant regulation with which the Company must comply;

5.2 In case where the Company has necessity to send or transfer the Personal Data to foreign countries, the destination country or the recipient of Personal Data must have the standard of Personal Data protection being equivalent to or higher than those in Thailand. In case where the destination country has the standard of Personal Data protection being lower or inadequate, the Company will send or transfer the Personal Data conforming to the provisions stipulated in the Personal Data Protection Act B.E. 2562 (2019). In addition, the Company will take action to establish the standard on security of the Personal Data as necessary and appropriate;

5.3 In case where the Company assigns or hires the external service provider or the Personal Data processor to process the Personal Data according to the Company's order or on behalf the Company, in such case, the Company will cause the external service provider or the Personal Data processor to provide the appropriate organizational measure, technical measure and physical measure to be in line with the standard of Personal Data Protection (i.e. there must be the entry into the Non-Disclosing Agreement: NDA; the Data Processing Agreement: DPA for controlling the operation of hires of the external service provider or the Personal Data processor to comply with the scope as prescribed in the Company's agreement or order);

5.4 In case where the Company accepts the transfer or shares the Personal Data from other agency to be used for Personal Data Processing, or in case where the Company transfers or shares the Personal Data to other agency, the Company will enter into the Data Sharing Agreement: DSA.

## **6. Personal Data Security Measures**

The Company sets up the appropriate security measures, comprising both technical and organizational measures and the appropriate physical measures in order to guarantee the confidentiality, accuracy, integrity, and availability of the Personal Data, and in order to prevent data loss, unauthorized or unlawful access, use, alteration, or disclosure of the Personal Data which are in line with the Information and Technology Policy of the Company.

Furthermore, the Company creates the awareness of the Personal Data protection to be fully acknowledged by the organization. The Company has formulated guidelines of practice in order to have security of collection, use or disclosure of the Personal Data for guaranteeing the confidentiality, accuracy, integrity, and availability of the Personal Data.

In case where the Company assigns the external agency or the third person to take action relating to the collection, use or disclosure of the Personal Data of the Data Subject in place of the Company, the Company will cause such external agency or the third person to provide appropriate security measure, for instance, storage of the Personal Data as confidentiality, to preserve the security of such Personal Data, and to prevent the Personal Data from being collected, used or disclosed for any other affair without authority or violating the law. In this connection, there must be the entry into agreement (specifying rights and duty, category of the Personal Data, purpose, scope of the collection, use or disclosure of the Personal Data including any other details in line with the form and standard prescribed by the Company) for controlling the operation of the external agency or the third person (who is assigned or hired to collect, use or disclose the Personal Data);

In case where the external agency or the third person (who is the Personal Data processor) further assigns the sub-service provider (for instance, the Sub- Personal Data processor) for the purpose of the collection, use or disclosure of the Personal Data, the Company will supervise such Personal Data processor to enter into the agreement between the Personal Data processor and the Sub-Personal Data processor.

## 7. Reporting of Personal Data Breach

In reporting the Personal Data Breach, the Company will take action as prescribed in the Notification of the Office of the Personal Data Protection Commission regarding Criteria and Method for Reporting Personal Data Breaches B.E.2565 (2022) (“**Notification**”), as follow:

When any person experiences the Personal Data Breach (or has doubt that such Personal Data Breach is a threat of Personal Data, such person must report such Personal Data Breach to the Data Protection Officer (“DPO”) by recording details in the Personal Data Breach Record Form prescribed by the Company. Such person must consider credibility of such Personal Data Breach and assess the impact from such Personal Data Breach.

To coordinate and contact the person who will analyze such Personal Data Breach for analyzing the cause of Personal Data Breach and to assess the impact and severity of such Personal Data Breach).

Next, DPO will discuss with the executive for giving advice and for setting the guideline of remedy for such Personal Data Breach and for taking any necessary action.

The Company will report such Personal Data Breach to the Office of the Personal Data Protection Commission (PDPC) within 72 hours as from the time that there is such report and confirmation of such Personal Data Breach, except there is no risk and impact to persons’ right and freedom from such Personal Data Breach. In case where such Personal Data Breach may cause high risk to persons’ right and freedom, the Company will report such Personal Data Breach to the Data Subject without delay.

In case where the Company must report such Personal Data Breach to the Office of the Personal Data Protection Commission (PDPC) and the Data Subject, the Company will report it in writing or will report by electronic mean or via any other means as determined by the Office of the Personal Data Protection Commission (PDPC). The report of such Personal Data Breach must contain the subject matter as much as practicable as follows:

- 1) Brief information about the nature and type of Personal Data Breach (there may be description of nature and number of the Data Subject or nature and number of items of Personal Data Breach);
- 2) Name, contact address and contact method of the Data Protection Officer;
- 3) Information about potential impacts from the Personal Data Breach;
- 4) Information about measures the Company has taken or will use to prevent, stop or correct such Personal Data Breach or to remedy such incident.

In case where the Company is unable to report such Personal Data Breach within 72 hours as from the time that there is such report and confirmation of such Personal Data Breach, the Company must give the reason, necessity of such delayed action together with the relevant details to show that there is the unavoidable necessity (which results in such delayed report of Personal Data Breach). However, the Company must report it to the Office of the Personal Data Protection Commission (PDPC) speedily but not exceeding 1 day as from the Company is aware of such Personal Data Breach.

In case where the Company reports the Personal Data Breach which may cause high risk to persons’ right and freedom, the Company will report such Personal Data Breach to the Data Subject (to acknowledge the incident together with the remedial measure including the preventive guideline).

In case where the Company must report the Personal Data Breach to the Data Subject, the Company must report by using the easily understandable and clear language as follow:

- 1) Brief information about the nature of Personal Data Breach;
- 2) Name, contact address and contact method of the Data Protection Officer;
- 3) Information about potential impacts to the Data Subject from the Personal Data Breach;
- 4) Remedial measures of the Data Subject including brief information about measures that the Company will use to prevent, stop or correct such Personal Data Breach or to remedy such incident, including advice regarding the additional measure which the Data Subject may take in order to prevent, stop or correct such Personal Data Breach.

## 8. Rights of the Data Subject

The Company respects the rights of the Data Subject as stipulated by law, therefore, the Company will take action according to the Data Subject's request for exercising his/her rights as stipulated in the Personal Data Protection Act B.E. 2562 (2019), in case where the Data Subject intends to exercise his/her rights via the channel: [www.aotga.com](http://www.aotga.com) or any other channels as prescribed by the Company. In this connection, the Data Subject has his/her rights according to the Personal Data Protection Law as follows:

**8.1 Right to withdraw the Consent.** The Data Subject is entitled to withdraw his/her consent of the Personal Data Processing at any time. However, such withdrawal of consent will not affect the Personal Data Processing whose consent has lawfully been given.

**8.2 Right to access the Personal Data.** The Data Subject is entitled to request access to the Personal Data where the Data Subject can notify the Company to prepare the copy of the Personal Data, and to request the disclosure of the acquisition of the Personal Data obtained without his/her consent.

**8.3 Right to Rectify the Personal Data to be accurate, up-to-date, complete, and not misleading.** The Data Subject has the right to ask the Company to rectify his/her Personal Data that are not accurate, complete or up-to-date so as to ensure that the Personal Data are accurate, up-to-date, and complete.

**8.4 Right to erase or destroy the Personal Data.** The Data Subject has the right to ask the Company to erase or destroy Personal Data or to make his/her Personal Data unidentifiable if the Data Subject finds that the Company has no necessity to retain such Personal Data according to the purpose for which they were collected, used or disclosed, or in case where the Data Subject has withdrawn the consent and the Company does not have authority to further collect, use or disclose such Personal Data, or in case where the Data Subject exercises the right to object the collection, use or disclosure of Personal Data and the Company has no ground to refuse such objection, or in case where the processing of such Personal Data is unlawful.

**8.5 Right to suspend the use of Personal Data.** The Data Subject has the right to suspend the use of his/her Personal Data in any of following circumstance:

- 1) During the period waiting for the Company to verify according to the Data Subject's request in order to correct his/her Personal Data to be accurate, complete and up-to-date;
- 2) When the Data Subject's Personal Data is collected use or disclosure unlawfully.
- 3) When his/her Personal Data is no longer required for retention in accordance with the necessary purposes as informed the Data Subject, but the Data Subject requests the Company to continue keeping that data for establishment, compliance with or to support the exercise of his/her legal claim;
- 4) At the time when the Company is proving to the Data Subject the superior lawful grounds, or collecting, using, or disclosing Data Subject's Personal Data is for establishing right of claim, compliance with or exercising of right, assertion of right of claim, or verifying the necessity of collecting, using, or disclosing Data Subject's Personal Data for public interest, due to the fact that Data Subject's has exercised his/her right to object to the collection, use, or disclosure of his/her Personal Data.

**8.6 Right to transfer the Personal Data.** The Data Subject has the right to request for the transfer of the Personal Data in case where the Company collects his/her Personal Data in a readable and commonly used, by automated devices or equipment, and can be used or disclosed by automated means. In this regard, the Data Subject shall have the rights as follow:

- 1) The Data Subject has the right to request for his/her Personal Data;

2) The Data Subject has the right to transfer his/her Personal Data in such formats to other Data Controllers

To exercise the above-mentioned right, it must be the case where the Data Subject has given consent to the Company for the collection, use, or disclosure of such Personal Data, or it must be the case where the Company collects, uses or discloses the Personal Data of the Data Subject in complying with the agreement to which the Data Subject is the contractual party, or for taking action according to the request of the Data Subject before entering into the agreement.

**8.7 Right to object the collection, use, or disclosure of the Personal Data.** The Data Subject has the right to object the collection, use, or disclosure of the Personal Data. In case where the Company processes the Data Subject's Personal Data for the lawful benefit of the Company, person or other juristic persons, or for performing the duties for the public interest or for the purpose of direct marketing, or for the purpose of scientific, historical or statistic research, except the Company has the lawful ground to refuse the Data Subject's request.

**8.8 Right to File the Complaint.** The Data Subject has the right to file a complaint to the Personal Data Protection Commission in case where the Company or the Processor of Personal Data of the Company including the officers, employees or contractors of the Company violates or does not comply with the Personal Data Protection Law. However, before filing the complaint, the Company would like to ask the Data Subject to contact the Company to enable the Company to have an opportunity to acknowledge the fact and to explain on various issues and to also ease the concern of the Data Subject first.

In case where the Data Subject requests for exercising such right, the Company will take action according to the process of management on the Data Subject's requests for exercising such right as follow:

The Company will take action according to the Data Subject's requests for exercising his/her right without unreasonable delay and the action will be completely taken within 30 days from the date of receipt of such request, or the receipt of complete supporting documents, as the case may be;

In case where the Company must deliver the Personal Data to the Data Subject, the Personal Data must be delivered in concise form, by using the easily understandable, easily accessed, clear and plain language.

In case where request for exercising his/her right is complicated or there is a lot of requests, the period for taking action on such requests may be extended not exceeding 60 days. In such case, the Company must notify the Data Subject to acknowledge such extension of time prior to the due 30-day period as from the date of receipt of such request.

In case where the Company refuses or being unable to comply with the Data Subject's request, the Company must immediately notify the Data Subject for acknowledgment immediately or within a maximum 30 days as from the date of receipt of such request together with the reason of refusal of the request. Moreover, the Company will notify the Data Subject to acknowledge his/her rights in filing complaint to the Personal Data Protection Commission and in exercising his/her rights in courts.

## **9. Disclosure regarding the Policy and Practice relating to the Personal Data**

The Company formulates the policy on the Personal Data Protection, practice of management of the Personal Data including the necessary measures for preserving the security of the Personal Data (which the Company collected, used, or disclosed according mission). In case where the Data Subject or the stakeholders have any doubt or wishes to acknowledge the details of practice relating to his/her Personal Data, the Data Subject can contact the Data Controller or the Data Protection Office according to the details as contained in Clause 12 of this Policy.

## 10. Employees' Duties and Responsibilities

The Company assigns its employees to emphasize and to be responsible for the collection, use or disclosure of the Personal Data and to strictly protect the Personal Data which the employees manage in accordance with the Personal Data Policy.

In case where the employees violate this Personal Data Protection Policy, they may suffer the disciplinary punishment.

## 11. Amendment of this Policy

The Company will consider to review this Personal Data Protection Policy from time to time. Such amendment will be published at [www.aotga.com](http://www.aotga.com) and other channels of the Company. However, if such amendment results in significant effect on the Data Subject as the owner of such Personal Data, the Company will notify the Data Subject to acknowledge such amendment in advance as appropriate before such amendment or correction is effective.

## 12. Contact Details

If you as the Data Subject wishes to contact the Company for inquiring or for exercising any rights regarding the Personal Data, you can contact

### 12.1 Data Controller: DC

**Company's Name:** AOT Ground Aviation Services Co., Ltd.

**Contact Address:** 222 Room 4326 4th Floor, Terminal 1, Don Mueang International Airport  
Vibhavadi-Rangsit Road, Sanambin Sub District, Don Mueang District,  
Bangkok

**Phone Number:** 063 898 3126

### 12.2 Data Protection Officer: DPO

**Contact Address:** 222 Room 4326 4th Floor, Terminal 1, Don Mueang International Airport  
Vibhavadi-Rangsit Road, Sanambin Sub District, Don Mueang District,  
Bangkok

**Email:** [dpo@aotga.com](mailto:dpo@aotga.com)

**Phone Number:** 063 898 3126

Announced on 27 January 2026

*(signature)*

(Mr. Siriwat Tovachirakul)  
President