Terms and Conditions in Personal Data Processing (DPA)

Whereas the Data Controller and the Data Processor have entered into an Agreement, and in performing obligations under such Agreement there are circumstances where the Data Processor must process Personal Data pursuant to the instructions of, or on behalf of, the Data Controller.

The Parties therefore agree to enter into these Terms and Conditions to govern and carry out the processing of Personal Data in compliance with Personal Data Protection Laws, with the following terms:

1. Definitions and Interpretation

1.1 "**Agreement**" means any contract, agreement, or juristic act relating to Personal Data Processing activities.

1.2 "**Personal Data**" means any information relating to a natural person which enables the identification of such natural person, whether directly or indirectly, which may be:

(a) collected directly from the Data Subject;

(b) disclosed to the Data Processor or its personnel by the Data Controller, its personnel, or the Data Controller's Affiliates who are involved, concerned with, or required to be involved in the performance under the Agreement; or

(c) disclosed to a Sub-Processor or its personnel by the Data Processor, its personnel, or the Data Processor's Affiliates who are involved, concerned with, or required to be involved in the performance on behalf of the Data Processor.

For the avoidance of doubt, Personal Data does not include information of deceased persons.

1.3 "**Data Controller**" means Advanced Info Service Public Company Limited ("AIS") and/or its Affiliates that enter into the Agreement with the Data Processor, having the authority to make decisions regarding the collection, use, or disclosure of Personal Data.

1.4 "**Data Processor**" means a person or juristic person that enters into the Agreement with the Data Controller and performs the collection, use, or disclosure of Personal Data pursuant to the instructions of, or on behalf of, the Data Controller, and is not a Data Controller in doing so.

1.5 "**Sub-Processor**" means a person or juristic person engaged or subcontracted by the Data Processor to perform Personal Data Processing.

1.6 "**Personal Data Processing**" means any operation relating to the collection, use, or disclosure of Personal Data, including recording, arranging, combining, organizing, storing, structuring, modifying, using, restricting, deleting, destroying, transferring or forwarding (both domestically and cross-border), publishing, disclosing, or accessing, in each case by any means, as instructed by the Data Controller for the purposes of the Agreement.

1.7 "**Data Subject**" means a natural person who can be identified, directly or indirectly, from the Personal Data.

1.8 "**Personal Data Protection Laws**" means the Personal Data Protection Act B.E. 2562 (2019), including any rules, regulations, notifications, announcements, or other subordinate legislation issued thereunder, and any other applicable laws relating to personal data protection (as amended and/or replaced from time to time), as well as personal data protection laws of other countries applicable to the Personal Data under these Terms and Conditions.

1.9 "**Affiliates**" of each Party means any juristic person under the control of such Party, any juristic person having control over such Party, or any other juristic person under the common control of the same controlling juristic person.

1.10 "**Log File Data**" means data relating to computer system communications indicating the source, origin, destination, route, time, date, volume, duration, type of service, or any other information relating to such computer system communications.

1.11 "**Personal Data Breach**" means a breach of security measures causing the loss, access, use, alteration, modification, or disclosure of Personal Data without authority or unlawfully, whether resulting from intentional acts, willful misconduct, negligence, unauthorized acts, computer offenses, cyber threats, defects, accidents, or any other causes.

1.12 **"Artificial Intelligence" or "AI"** means any system, technology, or model designed or developed to infer from inputs in order to generate outputs, such as predictions, content, recommendations, or decisions, in accordance with specified objectives.

2. Responsibilities of the Data Processor

2.1 The Data Processor shall comply with the Personal Data Protection Laws and process Personal Data only in accordance with the Principal Agreement and the documented instructions of the Data Controller. If the Data Processor considers that any instruction of the Data Controller would result in a Personal Data Breach or contravene the Personal Data Protection Laws, the Data Processor shall immediately notify the Data Controller and propose alternative processing methods. If the Data Processor fails to comply with this Clause 2.1, the Data Processor shall be deemed to act as a Data Controller in respect of the relevant Processing.

2.2 The Data Processor warrants that access to Personal Data shall be limited only to individuals necessary for Personal Data Processing under the Agreement and solely as necessary to comply with the Data Controller's instructions.

2.3 The Data Processor shall supervise its personnel, employees, agents, and/or Sub-Processors to ensure that the processing of Personal Data is carried out in accordance with the instructions and requirements of the Data Controller. The Data Processor shall further ensure that such persons maintain the confidentiality of Personal Data and comply with security obligations at a level equivalent to those imposed on the Data Processor under these Terms and Conditions.

2.4 The Data Processor shall prepare and maintain records of processing activities, whether in documentary or electronic form ("Records"), throughout the term of the Agreement in accordance with the requirements of the applicable Personal Data Protection Laws and shall deliver such Records to

the Data Controller within seven (7) days upon request at any time or upon termination of the Agreement, as the case may be.

2.5 During the term of the Agreement, the Data Processor shall retain Log File Data for ninety (90) days from the date such data enters its computer system and shall delete or destroy such data immediately upon the expiry of such retention period.

2.6 The Data Processor shall implement appropriate security measures for Personal Data, taking into account the level of risk according to the nature, scope, and purposes of the services and/or activities under the Agreement, as well as the likelihood and potential impact of any Personal Data Breach. Such security measures shall be in compliance with the Personal Data Protection Laws and shall meet standards no less than those prescribed in the Notification of the Personal Data Protection Committee regarding the Security Measures of the Data Controller B.E. 2565 (2022). The Data Processor shall also implement cyber security measures that are equivalent to or no less stringent than the Cyber Security Standard for Third Parties, as set out at:
https://aisprocurement.cloud.ais.th/en/sustainable-supplier-development/cyber-security-standard

3. Governance of Artificial Intelligence

The Data Processor shall not Process Personal Data using, through, or in conjunction with any Artificial Intelligence ("AI") or any similar technology, whether such AI is operated by the Data Processor or any third party, unless the Data Processor has obtained the Data Controller's prior written consent.

Where such consent has been granted, the Data Processor shall process Personal Data using AI solely in accordance with the instructions, purposes, scope, and conditions specified by the Data Controller. The Data Processor shall not use any Personal Data, prompts, outputs, or any data derived from such processing for the purpose of training, fine-tuning, developing, improving, testing, evaluating, or enhancing any AI or AI model of the Data Processor or any third party, whether directly or indirectly, unless the Data Controller has provided its specific prior written consent to such use.

4. Personal Data Breach Notification

4.1 The Data Processor shall notify the Data Controller in writing within 24 hours of becoming aware of a Personal Data Breach, cyber threat, or computer-related offense, and shall fully cooperate in investigation, mitigation, and remedy.

4.2 The Data Processor shall assist the Data Controller in reviewing security measures and mitigating impacts arising from each Personal Data Breach.

5. Sub-Processing

The Data Processor shall not appoint a Sub-Processor without prior written approval from the Data Controller. The Data Processor shall enter into a written agreement with the Sub-Processor with obligations no less protective than these Terms and Conditions and remains liable for the Sub-Processor's performance.

6. Rights of Data Subjects

6.1 The Data Processor shall promptly notify the Data Controller upon receiving any request from a Data Subject under the applicable Personal Data Protection Laws and shall cooperate with the Data Controller to enable it to respond to such request. The Data Processor shall not act on any Data Subject request on its own unless expressly instructed in writing by the Data Controller.

6.2 The Data Processor shall provide reasonable assistance to the Data Controller in handling complaints, investigations, or inquiries from competent authorities related to compliance with Personal Data Protection Laws or any other applicable laws and shall cooperate as necessary to allow the Data Controller to continuously verify that the Data Processor is complying with these Terms and Conditions.

7. Compensation for Damages

The Data Processor shall indemnify and hold harmless the Data Controller, Data Subjects, or any other persons for any claims, penalties, liabilities, fines, damages, or costs arising from or in connection with any breach of these Terms and Conditions or any Personal Data Breach, up to the amount of actual damages, and within the timeframe specified by the Data Controller.

8. Data Protection Impact Assessment

The Data Processor shall assist the Data Controller in conducting Data Protection Impact Assessments as required by applicable law, taking into account the nature of the processing, the processing methods, and the Personal Data involved in each assessment.

9. Deletion or Return of Personal Data

9.1 The Data Processor shall return, delete, or destroy all Personal Data, including any copies, within seven (7) business days from the termination of the Agreement or upon instruction of the Data Controller. In the event that a Data Subject terminates a contract with the Data Controller, the Data Processor shall delete the Personal Data immediately, or within ninety (90) days if necessary, unless retention is required by law or government order.

9.2 The Data Processor shall provide a certificate of completion to the Data Controller within seven (7) business days after completing the actions under Clause 9.1.

10. Audit Rights

The Data Processor shall provide all necessary information to demonstrate compliance with these Terms and Conditions and shall permit the Data Controller, or any auditor appointed by the Data Controller, to audit the processing, deletion, or return of Personal Data performed by the Data Processor, its Affiliates, or any Sub-Processors.

11. Transfer of Personal Data

The Data Processor shall not transfer Personal Data outside Thailand without the prior written consent of the Data Controller. If such transfer is necessary, the Data Processor shall ensure that the destination country or international organization has adequate data protection standards and shall implement appropriate safeguards in compliance with the Personal Data Protection Laws.

12. Integration with the Agreement

These Terms and Conditions shall form an integral part of the Agreement. Any breach of these Terms and Conditions by the Data Processor shall be deemed a breach of the Agreement, and the Data Controller shall have the right to terminate the Agreement and immediately claim all damages.