**[Template clauses for data processing where the Company has an existing service agreement with the data processor]**

**Amendment Agreement**

This Amendment Agreement (the "**Amendment**") is entered on [date] by and between [insert the company name] (the "**Company**") and [insert the data processor's company name] (the "**Service Provider**"), to amend [insert name of an existing service agreement] dated [insert date of an existing service agreement] between the Company and the Service Provider (the "**Service Agreement**").

The Company and the Service Provider are each hereinafter individually referred to as a "**Party**" and collectively referred to as the "**Parties**."

Capitalized terms not otherwise defined herein shall have those meanings ascribed to them in the Service Agreement.

The Parties agree to add a new schedule (Data Processing Requirements) attached herewith as Schedule [insert Schedule Number] to the Service Agreement.

This Amendment supersedes any contrary prior agreements, understandings, representations, undertakings, or negotiations, whether written or oral, between the Parties with respect to the subject matter herein.

Save as amended by this Amendment, the provisions of the Service Agreement shall continue in full force and effect.

**In witness whereof**, the Parties have entered this Amendment as of the date first written above.

[Insert the Company's name]

By: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Name:

Title:

[Insert the data processor's company name]

By: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Name:

Title:

**Schedule [insert Schedule Number] - Data Processing Requirements**

Where the Service Provider processes Personal Data (defined below) created, collected, or received to perform any services under the Service Agreement, the Parties agree that the terms of this Schedule [insert Schedule Number] shall apply. In the event of any inconsistency between this Schedule [insert Schedule Number] and the Service Agreement, the terms of this Schedule [insert Schedule Number] shall prevail and govern.

* + 1. Capitalized terms used herein shall have the meanings set forth in this Schedule [insert Schedule Number] or in the Service Agreement.

"**Data Protection Laws**" means all laws, regulations, and other legal requirements, including but not limited to the Personal Data Protection Act, B.E. 2562 (2019) and its sub-regulations (the "**PDPA**"), official guideline and interpretation thereof, as applicable to the processing of Personal Data (as amended and/or replaced from time to time).

"**Process**" shall mean any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as the collection, recording, organization, storage, adaptation, alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, cross-border transfer, alignment or combination, blocking, erasure, or destruction of the Personal Data.

In this Schedule [insert Schedule Number], the terms "**Personal Data**," "**Data Processor**," "**Data Subject**," and "**Data Controller**" shall have the meaning as defined in the Data Protection Laws.

* + 1. The Company shall be the Data Controller and the Service Provider shall be the Data Processor in respect of Personal Data processed by the Service Provider on the Company's behalf or at the Company's instructions in performing the Service Provider's obligations under the Service Agreement (the "**Company's Personal Data**").
    2. The Company shall be solely entitled to determining the purposes and means for which and the manner in which Personal Data is to be processed by the Service Provider in performance of the Service Provider's obligation under the Service Agreement. Where the Service Provider processes Personal Data on behalf of the Company or upon the Company's instructions, the Service Provider shall, in respect of such Personal Data:
       1. not process the Company's Personal Data for any purpose other than for the provision of services to the Company under the Service Agreement;
       2. act only on [written] instructions and directions from the Company, and comply promptly with all such instructions and directions received from the Company from time to time;
       3. immediately notify the Company if any instruction or direction from the Company violates the Data Protection Laws although the Service Provider shall continue processing the Company's Personal Data in accordance with any such direction or instruction previously given by the Company unless the Company withdraws or amends the direction or instruction;
       4. not disclose the Company's Personal Data to any employee, director, agent, contractor, or affiliate of the Service Provider, or any third party, except as necessary for the performance of obligations under the Service Agreement on a need-to-know basis, or to comply with the applicable law; or with the Company's prior written approval;
       5. implement all appropriate technical and organizational measures, including any additional technical and organizational security measures as required by the Company from time to time upon written request:
          1. to protect the security and confidentiality of the Company's Personal Data;
          2. to protect the Company's Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorized processing, access, or disclosure; and
          3. as required under Data Protection Laws to ensure a level of security appropriate to the risk, including as appropriate: (a) the pseudonymization and encryption of the Company's Personal Data; (b) the ability to ensure the ongoing confidentiality, integrity, availability, and resilience of processing systems and services; (c) the ability to restore the availability and access to the Company's Personal Data in a timely manner; and (d) a process to regularly test, assess, and evaluate the effectiveness of technical and organizational measures to ensure and maintain security when processing the Company's Personal Data;
       6. notify the Company immediately of any request made by a Data Subject under Data Protection Laws in relation to or in connection with the Company's Personal Data, and if required by the Company, permit the Company to handle any such request and at all times cooperate with and assist the Company to ensure the Company's compliance with its obligations under the Data Protection Laws in relation to these requests, including in relation to the Data Subjects' exercise of their rights thereunder, and if the Company elects not to handle any Data Subject request, the Service Provider shall handle such request. In all cases, the Service Provider shall provide a copy to the Company of all the Company's Personal Data which it discloses to the Data Subject; and
       7. process the Company's Personal Data in accordance with the type of Personal Data, subject matter and duration, purpose and categories of Data Subject as set out in [Annex].
    3. The Service Provider shall, immediately and in any event within [12 hours] of becoming aware, promptly notify the Company in writing of any actual or suspected accidental, unlawful, or unauthorized destruction, loss, alteration, access to, disclosure of or processing of the Company's Personal Data or breach of the applicable security policy ("**Incident**"). Such a notice shall include reasonable details of the Incident including, without limitation: (i) a description of the Incident; (ii) likely consequences of the Incident; (iii) the number of data subjects affected, number of records affected, and types of records affected; and (iv) the measures taken or proposed to be taken to address the Incident, including measures to mitigate possible adverse effects. The Service Provider shall cooperate fully with any investigation regarding the Incident and take all necessary measures to limit further unauthorized access to, disclosure of or unauthorized processing of the Company's Personal Data in connection with the Incident.
    4. The Service Provider shall cooperate and provide the Company with such reasonable assistance as the Company requires in relation to any complaints made by Data Subjects, or any investigations or inquiries made by any competent authority relating to the Company's or the Service Provider's obligations under the Data Protection Laws.
    5. In relation to Personal Data processed by the Service Provider under this Service Agreement and this Schedule [insert Schedule Number], the Service Provider shall cooperate with the Company to the extent reasonably necessary to enable the Company to adequately discharge its responsibility as a Data Controller under the Data Protection Laws.
    6. If the Service Provider collects Personal Data on behalf of the Company, the Service Provider shall provide the information to the Data Subjects and obtain any consent required by the Company in relation to the Company's data processing.
    7. The Service Provider shall at all times comply with Data Protection Laws in connection with performance of its obligations under the Service Agreement and this Schedule [insert Schedule Number].
    8. The Service Provider shall provide such cooperation as the Company reasonably considers to be necessary to enable the Company to audit and verify the Service Provider's compliance with this Schedule [insert Schedule Number] from time to time. Cooperation may include assisting the Company in carrying out risk assessments of the Service Provider's data processing operations, in particular providing information about and permitting the Company to inspect those operations.
    9. The Service Provider shall not export the Company's Personal Data processed by the Service Provider pursuant to this Schedule [insert Schedule Number] outside Thailand without the prior written permission of the Company. When that permission is given, it will be conditional upon any export being done in compliance with the lawful cross-border transfer mechanism under the applicable laws including the Data Protection Laws. The Service Provider agrees to enter into any necessary agreement to comply with the law which applies on cross-border data transfers.
    10. Upon the termination or expiry of the Service Agreement, the Service Provider shall delete or destroy all the Company's Personal Data processed on behalf of the Company or return it to the Company, and the Service Provider shall delete and destroy existing copies of all such Company's Personal Data, solely except when it must be retained for legal compliance purposes.
    11. In no event may the Service Provider subcontract the processing of any of the Company's Personal Data without the prior written approval of the Company. Any approval will only be given for a specific subcontractor, and will be conditional upon the Service Provider having executed a written contract with the third party subcontractor which contains terms for the protection of the Company's Personal Data which are no less protective than the terms set out in this Schedule [insert Schedule Number]. For the avoidance of doubt, if the Service Provider engages a sub-processor (i.e. subcontractor), the Service Provider shall remain liable to the Company for the performance of the sub-processor's obligations under the Data Protection Laws or any acts or omissions of the sub-processor.
    12. The Service Provider shall ensure that any of the Service Provider's personnel who have access to Company's Personal Data are bound by the confidentiality obligations for the processing of the Company's Personal Data.
    13. The Service Provider shall maintain a written record of all processing activities carried out on behalf of the Company. This record shall be prepared and maintained pursuant to Data Protection Laws, and contain, at a minimum:
        1. the categories of processing to be carried out;
        2. the names and contact details of any subprocessors;
        3. the names and contact details of the subprocessors' data protection officers;
        4. details of data transfers to third countries or international organizations, and documentation of the suitable safeguards employed; and
        5. a general description of the technical and organizational security measures taken to safeguard the Personal Data.

The Service Provider shall provide this written record to the Company promptly upon request, and agrees that this record may be submitted by the Company to any third party data controller (as applicable) and to the relevant competent authorities.

* + 1. The Service Provider shall indemnify the Company against all fines, losses, or damages incurred by the Company as a result of the Service Provider's breach of this Schedule [insert Schedule Number], notwithstanding any limitation of liability under the Service Agreement.
    2. [The Parties acknowledge and agree that the Company may need to review and amend this Schedule [insert Schedule Number] if changes are required for the Service Provider to continue to process the Personal Data in compliance with the Data Protection Laws and to address the legal interpretation of the applicable laws including the Data Protection Laws. Therefore, the Parties shall discuss and agree in good faith any amendments required to this Schedule [insert Schedule Number].]

**Annex**

**Details of the Processing of Personal Data**

1. **The types of Personal Data to be processed**

[Insert list of data types]

1. **Subject matter**[[1]](#footnote-1) **and duration of the processing of the Company's Personal Data**

The subject matter and duration of the processing of the Company's Personal Data are set out in the Service Agreement and this Schedule [insert Schedule Number].

1. **Purposes of the processing of Personal Data**

[Insert]

1. **The categories of Data Subject to whom the Personal Data relates**

[Insert][[2]](#footnote-2)

1. **Special categories of data**

[Insert][[3]](#footnote-3)

1. [**BM**: For your information, "subject matter" refers to the subject matter of the main Service Agreement, e.g. cloud service as subject matter in the main Service Agreement.] [↑](#footnote-ref-1)
2. [**BM**: For example, potential customers, existing customers, employees.] [↑](#footnote-ref-2)
3. [**BM**: For example, race, ethnicity, religion from copy of national identification card, biometric data, facial recognition, fingerprints, health data from health and medical history/report, disability, criminal records.] [↑](#footnote-ref-3)